



STO TECHNICAL REPORT

TR-SAS-161-Vol-III

# **The NATO STO SAS-161 Research Task Group (RTG) – Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices Volume III: Comprehensive Defence, Capacity Building, and Enhanced Forward Presence**

(Le groupe de recherche (RTG) SAS-161 de la STO de l'OTAN –  
Aspects militaires de la lutte contre la guerre hybride :  
expériences, enseignements, meilleures pratiques  
Volume III : Défense complète, renforcement des capacités  
et meilleure présence militaire avancée)

This volume of SAS-161 presents case studies from  
Czechia, Great Britain, Latvia, Ukraine, and NSHQ,  
related to comprehensive defence, capability and  
capacity building, and enhanced forward presence.



Published October 2023





STO TECHNICAL REPORT

TR-SAS-161-Vol-III

# **The NATO STO SAS-161 Research Task Group (RTG) – Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices Volume III: Comprehensive Defence, Capacity Building, and Enhanced Forward Presence**

(Le groupe de recherche (RTG) SAS-161 de la STO de l'OTAN –  
Aspects militaires de la lutte contre la guerre hybride :  
expériences, enseignements, meilleures pratiques  
Volume III : Défense complète, renforcement des capacités  
et meilleure présence militaire avancée)

This volume of SAS-161 presents case studies from  
Czechia, Great Britain, Latvia, Ukraine, and NSHQ,  
related to comprehensive defence, capability and  
capacity building, and enhanced forward presence.

---

# The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published October 2023

Copyright © STO/NATO 2023  
All Rights Reserved

ISBN 978-92-837-2486-5

Single copies of this publication or of a part of it may be made for individual use only by those organisations or individuals in NATO Nations defined by the limitation notice printed on the front cover. The approval of the STO Information Management Systems Branch is required for more than one copy to be made or an extract included in another publication. Requests to do so should be sent to the address on the back cover.

# Table of Contents

	<b>Page</b>
<b>List of Figures</b>	<b>vi</b>
<b>List of Tables</b>	<b>vii</b>
<b>Acknowledgements</b>	<b>viii</b>
<b>SAS-161 Membership List</b>	<b>ix</b>
<b>Executive Summary and Synthèse</b>	<b>ES-1</b>
<b>Chapter 1 – Introduction</b>	<b>1-1</b>
1.1 Background	1-2
1.2 Method	1-2
1.3 Overview of Analysis	1-4
1.4 Topics Covered in this Volume	1-5
1.5 References	1-6
<b>Chapter 2 – SOF Support to Counter Hybrid Warfare: A Case Study of the NATO-Ukrainian Special Operations Forces Development Project</b>	<b>2-1</b>
2.1 Introduction	2-1
2.1.1 Research Methodology	2-1
2.2 Hybrid Warfare: An Evolving Concept for an Evolving Practice	2-2
2.2.1 Comprehensive Defence as a Method for Countering Hybrid Warfare	2-3
2.2.2 Conceptually Framing SOF’s Role in Counter Hybrid Warfare	2-3
2.2.3 Special Operations Forces in CHW: NATO Perspective	2-4
2.2.4 NATO’s Recognition of the Counter Hybrid Warfare – Capacity Building Nexus	2-5
2.2.5 Mandating Ukrainian SOF as a Counter Hybrid Actor	2-5
2.2.6 Ukrainian Capability Building Environment: Crowded Space	2-7
2.2.7 SOF Unity of Command	2-8
2.2.8 Forward Trajectory	2-11
2.3 Deductions and Conclusions	2-11
2.4 References	2-12
<b>Chapter 3 – Organization of Territorial Defence of Ukraine Under the Hybrid War with Russia</b>	<b>3-1</b>
3.1 Introduction	3-1
3.2 Levels of RF Hybrid Aggression	3-3
3.3 Territorial Defence of Ukraine	3-6
3.4 Territorial Defence Priorities	3-9

3.5	Conclusions	3-13
3.6	References	3-13
<b>Chapter 4 – Military Aspects of Hybrid Warfare: The United Kingdom and Operation Cabrit</b>		<b>4-1</b>
4.1	Introduction	4-1
4.2	The NATO Enhanced Forward Presence	4-1
4.3	Previous UK Deployments to Europe and CABRIT: Historical Context	4-2
4.4	From Crimea to CABRIT: Shaping the Mission	4-2
4.5	Experiences from CABRIT	4-3
4.6	The Importance of Cultural Links between Host Nations and Deployable Forces	4-4
4.7	Understanding Information Activities	4-6
4.8	Military Perspectives for the Future	4-8
4.9	Conclusions, Key Takeaways, and Lessons for Others	4-9
4.10	References	4-10
<b>Chapter 5 – Case Study of Russian Hybrid Activities in the Czech Republic</b>		<b>5-1</b>
5.1	Strategic Approach of the Russian Federation when Using “Hybrid Influence”	5-1
5.1.1	Comprehensive Cross-Domain Approach	5-1
5.1.2	Cyber Influence	5-3
5.1.3	Information Operations	5-5
5.1.4	The Operation of Intelligence Services and Political and Economic Influence	5-7
5.2	Proposals, Recommendations and Implications	5-9
5.2.1	Proposals and Recommendations in the Construction and Strengthening of Resilience in the Czech Republic	5-9
5.2.1.1	Coordination	5-9
5.2.1.2	Updating the Conceptual, Doctrinal and Legislative Framework	5-10
5.2.1.3	Strengthening the Resilience of Society, the State and Critical Infrastructure	5-10
5.2.1.4	Proactive Approach	5-11
5.2.2	Proposals and Recommendations for the Armed Forces of the Czech Republic	5-11
5.3	References	5-12
<b>Chapter 6 – Russia’s Influence Operations in the Baltic States</b>		<b>6-1</b>
6.1	Introduction	6-1
6.2	Russia and the Baltic States: Finlandization	6-2
6.3	Political	6-5
6.4	Economic and Social	6-9
6.5	Diplomatic and Informational	6-10

---

6.6	Energy	6-11
6.7	Final Remarks	6-12
6.8	References	6-13
<b>Chapter 7 – Conclusion</b>		<b>7-1</b>
<b>Annex A – Table of Implications – Source Material</b>		<b>A-1</b>

---

## List of Figures

<b>Figure</b>		<b>Page</b>
Figure 3-1	Elements of the Hybrid War of the Russian Federation Against Ukraine	3-2
Figure 3-2	The Structure of the State TrD (Option)	3-12
Figure 5-1	The Total Number of Articles about Vrbetice Published Daily in the Observed Period in Czech (Yellow), English (Blue) and Russian (Red)	5-7
Figure 6-1	Trust in Political Institutions in the Baltic Region	6-4



---

## List of Tables

<b>Table</b>		<b>Page</b>
Table 3-1	The Sequence of the Main Measures of the Russian Hybrid Aggression Against Ukraine	3-4
Table 3-2	Comparative Analysis of the Results of Local Elections in 2015 and 2020 in the Four Southern Regions of Ukraine	3-8

---

## Acknowledgements

The SAS-161 RTG could not have conducted its work, particularly through the challenges of the pandemic and then, for our Ukrainian members, in the face of the existential threat created by Russia's full invasion of their country, without the support of many people. The NATO Liaison Office Kyiv facilitated the initial translation of Volume I from Ukrainian to English. The NATO STO Collaboration Support Office (CSO) in Paris, the staff at the Political Affairs & Security Policy Division in Brussels, the NSHQ J9 Staff in Mons, and staff at Defence Research and Development Canada, Centre for Operational Research and Analysis (DRDC CORA) in Ottawa, and the staff of the Croatian Defence Academy "Dr. Franjo Tuđman", in Zagreb all provided the support required for the RTG to conduct the meetings demanded by our work program. The Zagreb Security Forum (ZSF), led by RTG member Dr. Gordan Akrap, created the opportunity to present preliminary results at the October 2022 ZSF. The ZSF is truly a superb platform for forthright discussion of important and sensitive topics. Ukraine has proven, once again, to be an ideal scientific collaborator and we thank the National Defence University of Ukraine and the NATO-Ukraine Platform for Countering Hybrid Threats for sponsoring this collaboration and assisting in the travel of our Ukrainian members.

# SAS-161 Membership List

## CO-CHAIRS

Mr. Neil CHUKA\*  
Defence Research and Development Canada CORA  
CANADA  
Email: [NEIL.CHUKA@forces.gc.ca](mailto:NEIL.CHUKA@forces.gc.ca)

Col Dr. Viacheslav SEMENENKO\*†  
National Defence University of Ukraine  
UKRAINE  
Email: [semenenko17viacheslav@gmail.com](mailto:semenenko17viacheslav@gmail.com)

## MEMBERS

Assist. Prof. Gordan AKRAP  
Hybrid Warfare Research Institute  
CROATIA  
Email: [gakrap@yahoo.de](mailto:gakrap@yahoo.de)

Mr. Matthew LAUDER  
DRDC  
CANADA  
Email: [Matthew.Lauder2@ecn.forces.gc.ca](mailto:Matthew.Lauder2@ecn.forces.gc.ca)

Ms. Dorthe BACH NYEMANN  
Royal Danish Defence College  
DENMARK  
Email: [dony@fak.dk](mailto:dony@fak.dk)

Cpt. (ret.) Ivica MANDIĆ  
St. George Association  
CROATIA  
Email: [vcmandc@gmail.com](mailto:vcmandc@gmail.com)

Dr. Jānis BĒRZINŠ\*  
National Defense Academy of Latvia  
LATVIA  
Email: [janis.berzins01@mil.lv](mailto:janis.berzins01@mil.lv)

Col. Janne MÄKITALO  
Finnish Army Academy  
FINLAND  
Email: [janne.m.makitalo@mil.fi](mailto:janne.m.makitalo@mil.fi)

Dr. Jan BREN\*  
Centre for Security and Military Strategic Studies  
CZECHIA  
Email: [jan.bren@unob.cz](mailto:jan.bren@unob.cz)

Mr. Giles READER\*  
Dstl  
UNITED KINGDOM  
Email: [greader@dstl.gov.uk](mailto:greader@dstl.gov.uk)

Dr. Byron HARPER\*  
Allied Special Operations Forces Command  
Deputy, J9 Partnership Division  
Email: [byron.harper@nshq.nato.int](mailto:byron.harper@nshq.nato.int)

Ms. Jeanette SERRITZLEV  
Royal Danish Defence College  
DENMARK  
Email: [jese@fak.dk](mailto:jese@fak.dk)

Ms. Linda JARL  
Swedish Defence Research Agency (FOI)  
SWEDEN  
Email: [linda.jarl@foi.se](mailto:linda.jarl@foi.se)

---

\* Contributing or supporting author of Volume III, Comprehensive Defence, Capacity Building, and Enhanced Forward Presence.

† Ukraine Project Lead

## **ADDITIONAL CONTRIBUTORS**

Mr. Petr MATOUS  
Czech Ministry of Defence  
CZECHIA

## **PANEL/GROUP MENTOR**

Mr. Sean BOURDON  
Defence Research and Development Canada CORA  
CANADA  
Email: [sean.bourdon@forces.gc.ca](mailto:sean.bourdon@forces.gc.ca)

# **The NATO STO SAS-161 Research Task Group (RTG) – Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices**

## **Volume III: Comprehensive Defence, Capacity Building, and Enhanced Forward Presence**

**(STO-TR-SAS-161-Vol-III)**

### **Executive Summary**

The NATO STO SAS-161 Research Task Group (RTG) investigating “Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices” is meant to inform the full spectrum of military planning at the Alliance and national level. This functionally oriented analysis touches all aspects of military effectiveness and help inform our collective efforts to account for the challenges of contemporary, and expected future characteristics, of competition, conflict, warfare, and warfighting.

With a focus on contributing to the long-term military effectiveness of the Alliance, Ukraine, and the individual Ally and Partner nations, the RTG applied the fundamentals of net assessment in developing two distinct research streams. Both research streams study contemporary Russian behaviors related to competition, conflict, warfare, and warfighting. The first stream further investigates, from Ukraine’s perspective, Russian aggression against Ukraine and Ukrainian institutional responses and preparations up to the full-scale invasion by Russia on 24 February 2022. The second research stream, undertaken by the non-Ukrainian members of the RTG, develops national or mission-specific case studies investigating Russian behaviors within differing contexts. The intent of this second stream is to identify military-specific aspects of those behaviors. The analysis and deductions related to each research stream are then combined and distilled into military implications.

The case studies presented in this volume highlight a number of important planning considerations for the Alliance and its partners. First, national level legal frameworks must be relevant to contemporary and expected future conditions of the operational environment. This is foundational as it sets the conditions for Alliance members and partners to contribute relevant and credible national capabilities to collective security and defence. Second, Russia will tailor its behaviors to the context of individual national targets. As both Bērziņš and Reader show, this might lead to targeting paths that are incongruent with national planning assumptions. Third, collectively, the case studies suggest that a major conclusion of the SAS-121 analysis – that Ukraine’s national context presented unique opportunities for Russian exploitation – remains valid. While some socio-cultural factors are shared with other Eastern European nations (e.g., ethnic Russian communities or Russian-speaking enclaves), each must be considered within individual national contexts. Fourth, Alliance support to partners must be coordinated and deconflicted and include, as much as possible, non-Alliance countries that are also seeking to contribute to partner nation capability and capacity development. Finally, the case studies reinforce that collective security and defence is only as strong as the national level arrangements that form the foundations of deterrence. Gaps at the national level, for both Alliance and like-minded partners, will undermine the whole. In this regard, national conceptions of total or comprehensive defence, aligned with relevant legal and policy frameworks, are critical. Holistic national approaches to security and defence are the foundation for effective counters to expected Russian behavior.

# **Le groupe de recherche (RTG) SAS-161 de la STO de l'OTAN – Aspects militaires de la lutte contre la guerre hybride : expériences, enseignements, meilleures pratiques**

## **Volume III : Défense complète, renforcement des capacités et meilleure présence militaire avancée**

**(STO-TR-SAS-161-Vol-III)**

### **Synthèse**

Le groupe de recherche (RTG) SAS-161 de la STO de l'OTAN – « Aspects militaires de la lutte contre la guerre hybride : expériences, enseignements, meilleures pratiques » vise à éclairer tout le spectre de la planification militaire au niveau de l'Alliance et au niveau national. Cette analyse fonctionnelle aborde tous les aspects de l'efficacité militaire et éclaire nos efforts collectifs visant à tenir compte des caractéristiques actuelles et futures (prévues) de la concurrence, des conflits, de la guerre et des combats.

En se concentrant sur la contribution à l'efficacité militaire à long terme de l'Alliance, de l'Ukraine et des pays alliés et partenaires, le RTG a appliqué les principes fondamentaux de l'évaluation nette pour établir deux axes de recherche distincts. Les deux axes de recherche étudient les actuels comportements russes liés à la concurrence, aux conflits, à la guerre et aux combats. Le premier axe étudie plus en détail, du point de vue de l'Ukraine, l'agression de la Russie contre l'Ukraine et les préparatifs et réponses institutionnelles de l'Ukraine jusqu'à l'invasion à grande échelle par la Russie le 24 février 2022. Le deuxième axe, suivi par les membres non ukrainiens du RTG, développe des études de cas nationales ou propres à une mission, qui examinent les comportements russes dans différents contextes. L'objectif de ce deuxième axe est d'identifier les aspects spécifiquement militaires de ces comportements. L'analyse et les déductions liées à chaque axe de recherche sont ensuite combinées et aboutissent à des implications militaires.

Les études de cas présentées dans ce volume mettent en évidence un certain nombre de considérations de planification importantes pour l'Alliance et ses partenaires. Premièrement, les cadres juridiques nationaux doivent être pertinents dans les conditions actuelles et futures (prévues) de l'environnement opérationnel. Cet aspect est fondamental, car il permet aux membres et partenaires de l'Alliance de contribuer de manière pertinente et crédible aux capacités collectives de sécurité et de défense. Deuxièmement, la Russie adaptera ses comportements au contexte de chaque objectif national. Comme Bērziņš et Reader le montrent, cela pourrait conduire à des chemins de détermination des objectifs qui ne correspondent pas aux hypothèses de planification nationales. Troisièmement, dans leur ensemble, les études de cas suggèrent qu'une conclusion majeure de l'analyse du SAS-121 – à savoir, que le contexte national de l'Ukraine présentait des opportunités uniques d'exploitation par la Russie – reste valable. Bien que certains facteurs socioculturels soient présents dans d'autres pays d'Europe de l'Est (par ex., des communautés ethniques russes ou des enclaves russophones), chacun d'entre eux doit être considéré dans le contexte national concerné. Quatrièmement, le soutien de l'Alliance aux partenaires doit être coordonné et dépourvu de conflit et inclure, autant que faire se peut, des pays non alliés qui cherchent également à contribuer au développement des capacités des pays partenaires. Enfin, les études de cas soulignent que la sécurité

et la défense collectives dépendent des arrangements nationaux qui forment les bases de la dissuasion. Les lacunes nationales, aussi bien dans l'Alliance que chez les partenaires partageant les mêmes idées, sont autant de points faibles qui sapent l'ensemble. À cet égard, il est essentiel de disposer de conceptions nationales de défense totale ou complète, en adéquation avec des cadres juridiques et politiques pertinents. Les démarches nationales holistiques de la sécurité et de la défense constituent la base de ripostes efficaces au comportement russe attendu.





## Chapter 1 – INTRODUCTION

Neil CHUKA

Defence Research and Development Canada  
CANADA

The NATO STO SAS-161 Research Task Group (RTG) investigating “Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices” is meant to inform the full spectrum of military planning at the Alliance and national level. The functionally oriented analysis and the country-specific case studies developed by the RTG touch all aspects of military effectiveness and help inform our collective efforts to account for the challenges of contemporary, and expected future characteristics, of competition, conflict, warfare, and warfighting.

Defence scientific research and development activities must, in the first instance, seek to contribute to the military effectiveness of the forces they support. Military effectiveness is defined as:

*the proficiency with which armed forces convert resources into fighting power. A fully effective military is one that generates maximum combat power from the resources physically and politically available to it. The most important attribute of military effectiveness is the ability to adapt to the actual conditions of combat and conflict (vice those that were assumed would occur). Military effectiveness is comparative and can only be assessed against a likely opponent or a rigorous composite adversary through a pacing threats construct.<sup>1</sup>*

Military effectiveness has political, military-strategic, operational, and tactical level components and is inextricably tied to military learning, adaptation, and innovation.<sup>2</sup> As might be expected, military effectiveness is defined differently depending on the purpose of the individual scholar. While we ascribe to Williamson Murray and Alan Millet’s national and organizationally-focused construct, others have focused on the ability of military formations to generate, apply, and reconstitute combat power [6]. Still others apply notions of effectiveness at what we might call the service or environmental level (e.g., Army, Navy, Airforce, etc.) [7], [8]. Scholars have also applied Murray and Millet’s framework to assess gaps in tactical level military effectiveness as a means of correcting national level political, social, and military historiography [9]. Of greater, more recent frequency, many have built upon Murray and Millet and their individual and combined work investigating learning, adaptation, and military innovation to focus on the specifics of the intersection of technology, doctrine, organizational culture, and other factors, and the implications for military effectiveness in contemporary times [10], [11], [12], [13], [14], [15]. Regardless of the particular focus, all of these consider political (inclusive of socio-cultural, economic, and other national factors), military-strategic, operational, and tactical issues affecting the ability of the armed forces to achieve desired ends.

Notions of military effectiveness color the work of many scholars in several fields of study, even of the words “military effectiveness” are not explicitly used. Moreover, the use of the words “military effectiveness” by authors certainly predates the work of Murray and Millet but their framework has proven sufficiently resilient to stand the test of time and, even if used as a foil, been employed in multiple academic fields of study.<sup>3</sup> It is for this reason that we loosely apply the military effectiveness framework as a guide for the work of SAS-161. The framework is relatable to a substantial body of serious academic and professional literature, it provides an innate flexibility that enables the integration of a broad range of subjects and helps focus our analysis for a particular purpose – the provision of STO support to the NATO military instrument of power.

---

<sup>1</sup> The military effectiveness definitions employed here originate in Millett et al. [1] pp. 1-27. These were adapted specifically for force development and design purposes by Chuka [2] and Chuka and Neill [3].

<sup>2</sup> See for example the essays in Murray and Millett [4] and Murray [5].

<sup>3</sup> On predating, see for example Sutherland [16].

## **1.1 BACKGROUND**

The SAS-161 RTG is the second Systems and Analysis Studies (SAS) activity conducted in collaboration with Ukraine. During the period 2015 – 2017, the SAS-121 Research Specialist Team (RST) investigated in detail the Russian annexation of Crimea and the instigation of its campaign in Eastern Ukraine.<sup>4</sup> That collaborative research activity demonstrated the earnest, forthright desire of our Ukrainian partners to investigate Russian methods of conflict, warfare, and warfighting, share their experiences, and work closely with NATO. The intent of SAS-121 was to contribute to the study and learning of contemporary conflict and warfare to help collective efforts to address shared security and defence challenges.

SAS-161 follows in the path of SAS-121 by studying the military aspects of countering hybrid warfare to better understand individual and collective experiences, develop and share lessons, and identify best practice. This present work partnered the National Defence University of Ukraine (NDUU) with analysts from Canada, Croatia, Czech Republic, Denmark, Finland, Great Britain, Latvia, and Sweden, and NATO SOF HQ (NSHQ) via the SAS Panel and the STO Collaboration Support Office (CSO). The work was Co-Chaired by Canada and the NDUU. At the NDUU, the “Project Kalmius” team was led by the Ukrainian Co-Chair of SAS-161, Colonel Viacheslav Semenenko.

Our work has two distinct research streams, both focused on studying Russian behaviors related to competition, conflict, warfare, and warfighting. The first stream further investigates, from Ukraine’s perspective, Russian aggression against Ukraine and Ukrainian institutional responses and preparations *up to* the full-scale invasion by Russia in February 2022. The second research stream was undertaken by the non-Ukrainian members of the RTG and sees the development of national or mission-specific case studies investigating Russian behaviors in specific differing contexts. The intent of this second stream is to identify military-specific aspects and implications of that behavior.

## **1.2 METHOD**

Designed and approved in October 2019, the SAS-161 work program seeks to provide a unique contribution to the broader literature on “hybrid” or contemporary warfare by best exploiting the talents of, and the information available to, the RTG members, all of whom are involved in defence planning or professional military education systems at the national or Alliance level. In an effort to differentiate from some other portions of the very large, and growing, body of literature on hybrid warfare, the RTG work program was designed to adhere to the fundamentals of “net assessment” while striving to produce analysis focused on the aforementioned conception of military effectiveness.

Net assessment is the comparative analysis of military, technological, political, economic, and other factors governing the relative military capability of nations.<sup>5</sup> Its purpose is to identify problems and opportunities that deserve the attention of senior defence officials [19], p.9. Net assessment is a practice that applies distinctive perspectives to identify problems, including organizational and socio-bureaucratic behavior within specific contexts, as a means of determining meaningful balance of force estimates and plausible strategic interactions to inform decision making (adapted from Ref. [20]). A Net Assessment mindset works to strengthen critical thinking while countering received wisdom or group think and is most valuable where it fosters the provision of contested advice to decision makers. Most importantly, a net assessment mindset demands the study of ourselves and our adversaries both.

For military planning purposes, net assessment is focused on power relationships: it is a means of capturing and orienting decision makers to the exploration of strategic interactions – in all their complexity and variables – between and among actors in the operating environment as a way to expose gaps and opportunities. This allows

---

<sup>4</sup> The final report of that RST is entitled “Research Specialist Team on Hybrid Warfare: Ukraine Case Study” [17].

<sup>5</sup> The following three paragraphs are adapted from Ref. [18], pp.7-8.

analysts to better understand contexts and what constitutes relevant change in the strategic environment that affects military decision making.<sup>6</sup> As analysts, it also allows us, in fact forces us, to characterize the bounds of competitive military space. In support of an estimative process, net assessment frames military problems as strategic interactions as a way to think about choices and their impacts [23]. And it forces us to contain our analysis within the boundaries or parameters of a particular time period.

In this way, net assessment is an approach – a way of thinking – that incorporates all-source and inter-disciplinary material and recognizes the intellectual necessity of both nurturing and managing contested advice at an organizational level. Net assessment, therefore, is not only, potentially, a “capacity” or a “capability” as it has been recently described in various restricted distribution Alliance documentation.<sup>7</sup> As such, it is not surprising that organizations deal with it hesitantly, certain that it might be necessary, but uncertain as to how or why. For instance, the 2010 NATO Strategic Concept calls on the Alliance to ensure it is “at the front edge in assessing the security impact of emerging technologies, and that military planning takes the potential threats into account.” Such admonition calls out for comparative assessment in aid of pursuing the strategic objective of maintaining competitive advantage over potential adversaries – but of course does not explicitly refer to “net assessment” [24], p.17. Neither, then, is it surprising that net assessment is variously considered to be a product, a capability, a process, an intellectual construct and a methodology. Nonetheless, both analysts and practitioners should embrace net assessment as an organizational mindset or approach that works to strengthen critical thinking while countering received wisdom or “group think,” rather than pursue it as an “authoritative” singular endeavor or point of departure for planning.<sup>8</sup>

With this in mind, the SAS-161 work program is guided by relatively straightforward parameters comprised of three pillars.

The first pillar is the focus on the *military* aspects of contemporary competition, conflict, warfare, and warfighting. While political, economic, financial, and other factors are relevant to some of the individual studies comprising the SAS-161 body of work, those non-military factors are only considered insofar as required to understand their military implications within the context of a particular case study. This focus does not disregard the interplay between the military and other instruments of power; rather, we apply this focus to help identify gaps in military authorities, responsibilities, legal frameworks, and policy that are exposed during the research and analysis. This is critical as the SAS-161 work is conducted under the auspices of the Alliance’s Science and Technology Organization (STO) and therefore must contribute to the use, development of, and effectiveness of the military instrument of power.

The second pillar is that Russia, inclusive of proxies and others that might contribute to Russian goals, is the sole threat actor under consideration. While other threat actors might apply methods similar to those of Russia, adherence to the principles of net assessment means that each threat actor (and target – e.g., Ukraine or any of the states considered in our case studies) must be considered in their own context. Broadening the research and analysis to include other threat actors risks studying the methods rather than the actor – something that is arguably of limited utility for military planning purposes and, regardless, has been done by many others.<sup>9</sup>

---

<sup>6</sup> See Ref. [21], pp. 90-97. Gouré explains the relationship between net assessment and the development of competitive strategies, recognizing that there are several acceptable definitions and usages of “net assessment.” For an excellent discussion of the origins of net assessment and the role of Dr Andrew Marshall in its development and implementation see Ref. [22], pp. 611-644.

<sup>7</sup> There is very little Alliance documentation on this point that can be referenced in an unclassified publication. The author has participated in unclassified Alliance meetings where this point has been made by others.

<sup>8</sup> This should not be interpreted as a claim that comparative assessment does not occur naturally – as Cohen has observed, the appraisal of military balances “goes on all the time in the minds of decision-makers and their staffs” [25], p. 4. The argument we are making here is the importance of improving upon stale threat-agnostic capability based planning methods.

<sup>9</sup> See for example, Giannopoulos et al., “The Landscape of Hybrid Threats: A Conceptual Model” (Public Version), [26]. A public version of this document was produced in 2012. See also the Multinational Capability Development Campaign Countering Hybrid Warfare project and series of publications. A summary of that work is available at: MCDC CHW project [27].

The third and final pillar is the preference for contemporary primary source material in the research and analysis. As much as possible given the intent to work at the unclassified level, the members of the RTG employ original official documentation, interviews, and other similar material considered to be primary source. This requirement is meant to emphasize and exploit the specialized knowledge and perspective held by the RTG members and thereby distinguish from analysis conducted by, for example, that in some academic fields.

No single project can be comprehensive and SAS-161 is no exception to this rule. For example, there is limited detailed discussion of the use of space or cyber capabilities and the case studies are not intended to span all recent targets of Russian malevolence or those countries that fall within Russia's self-proclaimed sphere of interest. Nonetheless, our research and analysis contributes to the broader body of work on contemporary competition, conflict, and warfare and contributes to the effort to better understand ourselves and Russia as an adversary.

With these parameters, the case studies and the Ukrainian Project Kalmius research and analysis were developed independently under central direction and guidance from the Chairs. This approach maximized the disparate professional and educational backgrounds and perspectives of the RTG members.

The implications development process described in the "Military Implications" volume of our reporting was then used to distil the military implications from the collated main analytic deductions identified in each individual piece of work. Military implications are defined as:

*The implied consequences of credible deductions arrived at through the application of professional judgment. An implication should be actionable, without identifying courses of action, and relate to one or more capability components or enablers in order to inform military planning. For operational research and analysis, any implication is likely to affect multiple functional areas, can identify new requirements, validate current capability paths, or suggest capabilities of declining relevance. Implications must centre upon military effectiveness and credibility. (Adapted from Ref. [28])*

The implications development process allows for the identification of commonalities and contrasts across all of the main deductions, enabling the integration of the entire body of RTG scholarship into a whole.<sup>10</sup> The incorporation of an implications development process as a core portion of the work program reinforces our focus on the military aspects of hybrid approaches and the application of such methods by a specific threat actor (Russia). The result is a specific set of recommendations tailored to planning functions. Consequently, we remain within the scope and intent of the NATO STO SAS mandate, respectful of the role and authorities of those executing planning functions in NATO and national level headquarters and remain true to the framework of academic and professional literature on military effectiveness and net assessment that provided the intellectual guidance in the development of the RTG work program.

### 1.3 OVERVIEW OF ANALYSIS

The specific topics covered in this volume of SAS-161 reporting are detailed in the next section. Overall, however, there are some major deductions resulting from the work as a whole.

Ukraine provides an exemplar of military effectiveness grounded upon superb military adaptation and flexibility. The current effectiveness of Ukraine's armed forces is rooted in almost 9 years of work that has modernized and transformed Ukraine's conceptions of security and defence with the support of a wide variety of international partners. As with any situation, there is an historical and contemporary context that must be appreciated and accounted for but all those interested in security and defence affairs will do well to study Ukraine's actions to glean insight and lessons.

---

<sup>10</sup> A similar process assessed the results of the SAS-121 analysis from a NATO perspective. That work is captured in the SAS-127 final report entitled "Hybrid Warfare: Implications for NATO" [29].

The reporting confirms the imperative to study each threat in a way that respects the context of adversary decision making and the specifics of behaviors directed at each target. Conversely, each target of Russian malevolence must be studied to understand the historic and contemporary conditions that create both vulnerabilities and shields against the Russian threat. Even when faced with multiple threats it is important that each is understood individually before designing comprehensive responses. In other words, a net assessment mindset applied to threat-based planning will result in greater understanding of threat, strengths, vulnerabilities, and risk.

Our analysis helps to highlight that, at the national level, the concept of “total defence” or “comprehensive defence” (e.g., the idea that national security and defence must be seen as a whole-of-government and whole-of-civil society responsibility) is the foundation of military effectiveness, at least from a homeland defence perspective. This is because such conceptions of national defence help clarify the role of military forces in relation to other instruments of national power and, hopefully, contributes to high levels of military political effectiveness.<sup>11</sup>

Finally, despite the fact that much of the work of the SAS-161 RTG was conducted remotely, in a distributed fashion, first because of the pandemic and latterly because of the full-scale Russian invasion of Ukraine, collaborative projects such as this contribute to our ability to reach greater levels of understanding and improve our knowledge on contemporary security and defence challenges.

## 1.4 TOPICS COVERED IN THIS VOLUME

This volume of reporting from SAS-161 presents case studies focused on improving the understanding of ideas of comprehensive defence at the national level, Alliance capacity building activities supporting the development of comprehensive defence with partner countries, and lessons from forward posturing of Alliance military forces. Dr. Byron Harper discusses the NATO-Ukraine SOF development initiative to identify lessons for building counter hybrid warfare capability, with a particular emphasis on comprehensive defence. Colonel Viacheslav Semenenko and V.S. Frolov provide insight into the development of Ukraine’s Territorial Defence forces prior to the renewed Russian invasion of February 2022, including the importance of improved legal frameworks, careful consideration of local and regional sensitivities, and logical limits to Territorial Defence Force military capabilities to help ensure integration into regular force structures when required. Mr. Giles Reader discusses issues identified and lessons learned from the UK’s deployments to Estonia related to the Alliance’s Enhanced Forward Presence (Northeastern Flank). In doing so, he exposes some planning assumption fallacies regarding expected Russian behaviors. Dr. Jan Bren sheds light on some contemporary Russian application of hybrid methods against the Czech Republic and makes recommendations to better prepare for, and defend against, those activities. Finally, Dr. Janis Bērziņš discusses Russian hybrid methods as applied against the Baltic republics. These lattermost case studies reinforce the importance of understanding national strengths and vulnerabilities and the way Russia attempts to tailor its actions to that context. Annex A contains a table linking the military implications in Volume V of the SAS-161 reporting to the case studies. The abbreviations CZE, GBR, LAT, UKR, NSHQ, denote the case studies in this volume.

---

<sup>11</sup> Military Political Effectiveness is defined as: The effort to obtain resources for military activity in relation to the goals set by the polity and the proficiency in acquiring those resources. Resources consist of reliable access to financial support, a sufficient military-industrial base (including assured access), a sufficient quantity and quality of manpower, and control over conversion of those resources into military capabilities. Military political effectiveness hinges on a clear **understanding of national grand strategy**. This necessarily includes strong comprehension of vital national interests, the enduring and immediate threats to those interests, and a grasp of likely activities and tasks and the resources to carry out those activities and tasks to counter the threats to those interests.

**1.5 REFERENCES**

- [1] Millett, A., Murray, W., and Watman, K. “The Effectiveness of Military Organizations.” In A. Millett and W. Murray (eds.), *Military Effectiveness: Volume 1 The First World War*. New Edition, NY: Cambridge University Press, 1988/2010, pp. 1-27.
- [2] Chuka, C. “Learning From (Recent) History? An Assessment of CF Joint-Level Learning, Innovation, and Adaptation Activities.” DRDC CORA TM2013-048, Ottawa: DRDC, March 2012.
- [3] Chuka, N., and Neill, D. “A Research and Analysis Framework for a Strategic-Level Lessons Learned Process.” DRDC CORA TM 2011-210. Ottawa: DRDC, December 2011.
- [4] Murray W., and Millett, A. (eds.), *Military Innovation in the Interwar Period*. NY: Cambridge University Press, 1996/2007.
- [5] Murray, W. *Military Adaptation in War*. Alexandria VA: Institute for Defense Analysis, 2009.
- [6] Mansoor, P. *The GI Offensive in Europe: The Triumph of American Infantry Divisions, 1941 – 1945*. Lawrence: Kansas: University Press of Kansas, 1999.
- [7] Reese, R. *Why Stalin’s Soldiers Fought: The Red Army’s Military Effectiveness in World War II*, Lawrence, Kansas: University Press of Kentucky, 2011.
- [8] Hill, A. *The Red Army and the Second World War*. Cambridge UK: Cambridge University Press, 2020.
- [9] Harward, G. *Romania’s Holy War: Soldiers, Motivation, and the Holocaust*. Ithaca: Cornell University Press, 2021.
- [10] Marcus, R. *Israel’s Long War with Hezbollah: Military Innovation and Adaptation Under Fire*. Washington DC: Georgetown University Press, 2018.
- [11] Finkel, M. *On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield*. Stanford CA: Stanford University Press, 2011.
- [12] Mansoor, P., and Murray, W. (eds.), *The Culture of Military Organizations*. Cambridge: Cambridge University Press, 2019.
- [13] Jungdahl, A., and Macdonald, J. “Innovation Inhibitors in War: Overcoming Obstacles in the Pursuit of Military Effectiveness.” *Journal of Strategic Studies*, 38(4), 2015, pp 467-499.
- [14] DeVore, M. “Armaments After Autonomy: Military Adaptation and the Drive for Domestic Defence Industries.” *Journal of Strategic Studies*, 44(3), 2022, pp. 325-359.
- [15] Tomes, T. *Military Innovation and the Origins of the American Revolution in Military Affairs*. Unpublished doctoral dissertation, University of Maryland, 2004.
- [16] Sutherland, R.J. “Organization for Military Effectiveness.” ORD Informal Paper No. 66/P10, Ottawa: Department of National Defence Operational Research Division, May 1966.
- [17] NATO STO, “Research Specialist Team on Hybrid Warfare: Ukraine Case Study.” STO-TR-SAS-121, Neuilly-sur-Seine, France: NATO Science and Technology Organization, February 2018.

- [18] Chuka, N., and Archambault, P. “Improving Joint Force Development and Design: Applying Concept-Based, Threat-Informed Principles to NATO Capability Development.” DRDC-RDDC-2022-L052, Ottawa: DRDC, March 2022.
- [19] US DoD, DoD Directive 5111.11, “Director of Net Assessment.” 14 April 2020.
- [20] Bracken, P. “Net Assessment: A Practical Guide” Parameters, Spring 2006.
- [21] Gouré, D. “Overview of the Competitive Strategies Initiative.” in T.G. Mahnken (ed.), *Competitive Strategies for the 21st Century: Theory, History and Practice*, Stanford: Stanford University Press, 2012, pp. 90-97.
- [22] Adamsky, D. “The Art of Net Assessment and Uncovering Foreign Military Innovations: Lessons From Andrew W. Marshall’s Legacy.” *Journal of Strategic Studies*, 43(5), 2020, pp. 611-644.
- [23] Skypek, T. “Evaluating Military Balances Through the Lens of Net Assessment: History and Application.” *Journal of Military and Strategic Studies*, 12(2), Winter 2010, pp. 6-9.
- [24] *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. NATO: Brussels, November 2010.
- [25] Cohen, E. *Net Assessment: An American Approach*. Tel Aviv: Jaffee Center for Strategic Studies, April 1990.
- [26] Giannopoulos, G., Smith, H., and Theocharidou, M. *The Landscape of Hybrid Threats: A Conceptual Model (Public Version)*. European Commission, Ipsra, 2020.
- [27] Multinational Development Capability Campaign Countering Hybrid Warfare (MDCC CHW) Project. *Countering Hybrid Warfare postcard* (publishing.service.gov.uk) [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/783087/MCDC\\_Countering\\_Hybrid\\_Warfare\\_Postcard-web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/783087/MCDC_Countering_Hybrid_Warfare_Postcard-web.pdf) (Accessed April 2023).
- [28] Chuka, N., Archambault, P., Auger, A., Gladman, B., Robinson, E., Taylor, B., and Wallace, B. “Implications Development Framework.” DRDC-RDDC-2018-L167, Ottawa: DRDC, July 2018.
- [29] NATO STO. “Hybrid Warfare: Implications for NATO.” STO-TR-SAS-127. Neuilly-sur-Seine, France: NATO Science and Technology Organization, May 2018.





## **Chapter 2 – SOF SUPPORT TO COUNTER HYBRID WARFARE: A CASE STUDY OF THE NATO-UKRAINIAN SPECIAL OPERATIONS FORCES DEVELOPMENT PROJECT**

**Byron Harper**

Allied Special Operations Forces Command  
Deputy, J9 Partnership Division

### **2.1 INTRODUCTION**

Within the context of NATO's support for Ukraine's defence and security reforms, Special Operations Forces (SOF) are often trumpeted as a model of success [1]. NATO and Ukrainian officials both tend to admire the coherence with which Ukrainian SOF development was conducted in cooperation with Alliance SOF. NATO's positive impact on Ukrainian SOF development is commonly attributed to two factors. One is the tight knit transatlantic SOF network, bound in this case through the NATO Special Operations Headquarters (NSHQ) [2], [3].<sup>1</sup> Second, one of the three missions of SOF operating within NATO is to conduct Military Assistance (MA) [4]. MA, in the simplest of terms, is capacity building. Therefore, rationally, a tightly knit group of professionals accomplishing a mission they were designed to conduct is unsurprising.

However, this simplified explanation, while valid, fails to capture adequately the conditions under which SOF was conducting MA. When contextualised in terms of the strategic environment, an examination of NATO's support to the development of Ukrainian Special Operations Forces (UAFSOF) reveals a remarkable intersection of three practices: counter hybrid warfare, comprehensive defence, and partner capacity building [5].<sup>2</sup>

This case study thus uses the NATO-Ukraine SOF development initiative to identify lessons for building counter hybrid warfare capability, with a particular emphasis on comprehensive defence. To establish a common frame of reference, the chapter begins by explaining how the terms hybrid warfare and comprehensive defence are used within the study as well as the relationship between the two practices. Next follows a discussion on the nature of Allied SOF and its broadly accepted role in countering hybrid warfare. These framing discussions provide the foundation necessary to draw specific lessons from the NATO-Ukraine SOF capability development experience.

#### **2.1.1 Research Methodology**

This chapter supports NATO SAS-161: *Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices*. The research was designed to examine the following question: What counter hybrid warfare lessons, if any, can be drawn from the NATO-Ukraine SOF Development project? The researcher used the case study approach supported by participant-observer and unstructured interview research methods.

---

<sup>1</sup> NSHQ was reflagged as Allied Special Operations Forces Command immediately after this chapter was completed. See <https://www.nshq.nato.int/>. NSHQ is used throughout this chapter as it was employed throughout the period covered by the analysis [6].

<sup>2</sup> Within the defence and development sectors, the terms Building Partner Capacity and Building Partner Capability are sometimes used to distinguish between quantity and quality. However, the two terms are often applied interchangeably. This document follows the NATO trend of using "Capacity Building" as an overarching term, with no intent to distinguish the action from "Capability Building." When discussing the specific Ukrainian SOF case, the most common descriptor used will be "capability development."

Many of the details presented in this chapter are based on the author's first-hand experience or personal knowledge, having participated in the project from its inception. The author, therefore, took several steps to avoid cognitive bias. First, the chapter's foundation rests upon a thorough literature review. Written references proved most helpful in creating the study's conceptual framework, i.e., defining terms such as counter hybrid warfare and identifying SOF's role within it. On the other hand, open-source material specific to UAFSOF development has only recently begun to emerge within academic and media spheres, and much of this initial corpus lacks depth or is inaccurate. Thus, to further ensure academic integrity, the author conducted open-ended interviews with scores of Allies and Ukrainian personnel from all levels who were either directly engaged in UAFSOF development or otherwise involved in Ukrainian defence and security reforms. For security reasons, the report does not cite the interviews nor the names of personnel who provided their perspectives.

## **2.2 HYBRID WARFARE: AN EVOLVING CONCEPT FOR AN EVOLVING PRACTICE**

A root challenge to identifying SOF's role in countering hybrid warfare rests not only in a lack of agreement on appropriate applications of the military in the modern security environment but more fundamentally in the lack of an agreed definition of hybrid warfare [7]. According to the most prevalent descriptions, hybrid warfare is a method through which a belligerent state seeks to obfuscate its aggressive actions against a target nation. The offending party's objective is to coerce the target nation without provoking violent conflict. It achieves its goal through a carefully blended application of traditional and unconventional tools and tactics. If the aggressor is successful, the targeted nation either cannot recognise the threat or amass the evidence needed to mobilise the level of domestic and international support necessary to enact effective countermeasures. "*Political warfare*," "*competition below the threshold of war*," "*grey zone*" and "*left of bang*" are all equally fluid concepts within the hybrid warfare discourse [8].

On the conceptual level, the descriptions of hybrid warfare are easy to understand. However, among practitioners, identifying a commonly agreed, authoritative definition proves more challenging. This gap is attributable, in part, to the rapidly emerging and dynamic nature of hybrid warfare. Hybrid warfare practices continue to evolve, even as those affected by them strive to categorise hybrid activities as elements of international affairs.<sup>3</sup> Moreover, it is often difficult to discern between hybrid activity and artful statecraft.

Determining a definition is, nevertheless, important. As James Whither observes, "Defining hybrid warfare is not just an academic exercise. How the term is defined may determine how states perceive and respond to hybrid threats and which government agencies are involved in countering them" [9]. For instance, the Russian Federation's renewed assault on Ukraine brings to light the need for a defence policy decision on whether hybrid warfare ceases when open conflict ensues or if the conflict is simply a subset of a greater hybrid warfare campaign. Consider two options. The first option contends that Russia's 2008 invasion of Georgia, 2014 occupation of Eastern Ukraine and Crimea, and 2022 offensive against the whole of Ukraine are "traditional" military operations within a grander hybrid warfare campaign. According to option two, Russia failed to achieve their objectives through their preferred hybrid means. The second option would therefore conclude that Russia resorted to open warfare in response to an unsuccessful hybrid warfare campaign. The selected option will inform how states adapt their defence and security organisations to deter and defend against threats.

Rather than selecting a definition subject to the ongoing debate, this study identified four characteristics vital to the execution of hybrid warfare. First, the aggressor state blends legitimately recognised foreign affairs instruments and practices with actions outside accepted international norms, as codified in the customs, treaties, and institutions that define such norms. Second, hybrid warfare activities may include the threat or use of violence. However, violence is not a necessary component of hybrid warfare. Conversely, instruments

---

<sup>3</sup> As applied here, the term *international affairs* encompasses war, intelligence actions and diplomacy.

or actions offensively applied outside the norms of foreign affairs are, indeed, essential elements of hybrid warfare. Third, the aggressor state's success relies heavily on its ability to deny its actions. The ability to attribute hybrid activity (i.e., illegal, offensive actions) to the aggressor state increases the likelihood that the international community will implement measures designed to counteract or punish the aggressor. When the aggressor cannot plausibly deny its actions, it will seek to justify them within the framework of international laws and norms. These three characteristics enable the fourth and most important: the aggressor seeks to remain below the threshold of armed conflict where possible and isolate or minimise conflict when the threshold is breached.

Thus, for this case study, hybrid warfare is a method through which a belligerent state seeks to obfuscate aggressive actions it takes against a target nation, to avoid eliciting an effective response from the aggrieved or the international community.

### **2.2.1 Comprehensive Defence as a Method for Countering Hybrid Warfare**

Comprehensive Defence, as used in this study, is “an official government strategy, which encompasses a whole-of-society approach to protecting the nation against potential threats” [10]. Comprehensive defence naturally intersects with counter hybrid warfare in concept and practice. Conceptually, comprehensive defence is founded on the notion that only a small percentage of society is obligated to defend the nation against natural, accidental, or malicious acts. This notional “2%” of the population has a contractual obligation to serve the state at the municipal, regional, or national level. Thus, states that employ comprehensive defence seek to motivate and enable as much of the remaining 98% as possible to exercise their natural right to contribute to the nation's defence and security.

In practice, the comprehensive defence spectrum begins with individual resilience. As a result of state-provided education, training, and situational awareness programmes, “the 98%” (or some appreciable portion) is able and willing to protect itself if a threat were to manifest, be that through self-evacuation or basic survival [11]. By optimising individual resilience among the 98%, the nation disencumbers “the 2%” from tending to issues that do not truly require professional expertise during emergencies. At the other end of the comprehensive defence spectrum, willing and able members of the 98% actively participate in defence and security. The nature of individual participation will vary based on varying degrees of motivation and skill. Participation also depends on the nature of the threat or event; i.e., natural, accidental, or malicious.

When couched in terms of comprehensive defence, hybrid warfare tactics are malicious acts that do not crest the threshold of traditional war. Indeed, if the aggressor is successful, its actions will not be attributable to them and may not even be noticeably malicious. However, the outward appearance of a hybrid warfare tactic does not necessarily undermine comprehensive defence, as comprehensive defence is designed to protect society against all external threats, regardless of form. Thus, counter hybrid warfare is an inherent component of comprehensive defence.

### **2.2.2 Conceptually Framing SOF's Role in Counter Hybrid Warfare**

In 2016, the NATO Special Operations Headquarters, with the support of the U.S. Naval Postgraduate School (NPS), conducted an extensive study on extant and potential future roles for SOF in countering hybrid warfare “in a pre-Article V scenario.” Before reviewing the research, a brief discussion of the diverse pool from which the contributors were drawn provides a practical example of the so-called *Global SOF Network*. First, the organisation that sponsored the study, the NSHQ, is staffed by special operations personnel from thirty Allied and NATO Partner nations. Among its tasks, the NSHQ is responsible for delivering strategic-level special operations advice and support to NATO. Hence, the topic explored by the study is a subject of routine conversation within the headquarters and across the internationally aligned special operations community.

NPS, which contributed academic expertise, has been supporting research and conferring advanced degrees to military and civilian government officials since 1908. In the early 1990s, the school instituted a *Special Operations and Low-Intensity Conflict* track within its *Defense Analysis* programme [12]. The institution notes the diversity of its student body: “Since 1954, over 6500 International officers from more than 127 countries have graduated from NPS” [13].

The professional diversity and expertise common to the NSHQ and NPS were foundational to their joint study, the results of which were published in the November 2016 edition of the *Combating Terrorism Exchange* journal [14]. The article’s authors comprised a collection of fifteen academics and practitioners from six different nations: Denmark, Hungary, Norway, Türkiye, Ukraine, and the United States. The researchers were guided by a question posed by the NSHQ commander, “what courses of action can NATO, as an Alliance of 28 nations, take to counter or mitigate threats below the threshold of war, without requiring additional authorities beyond those currently approved by the North Atlantic Council, NATO’s governing body?” [15].

The research question resulted in a wealth of analysis, which is categorised according to “The Theory, History and Current State of Hybrid Warfare,” “Russian Hybrid Strategies and Tactics in Ukraine” and “NATO Responses to Hybrid Strategies.” Within the volume, two discussions prove particularly germane to this project. First, Espen Berg-Knutsen, the director of the Special Operations Research Development Program at Norway’s Defence Research Establishment (FFI), highlighted the relationship between counter hybrid warfare and unconventional warfare to frame SOF’s responsibilities within what he offers are inseparable undertakings [16]. In a separate article, three of Berg-Knutsen’s fellow Norwegians proposed an approach to military assistance that allows a providing nation to contribute to deterrence, while simultaneously creating tangible, enduring capabilities, both at home and within a partner nation [17]. SOF’s roles in comprehensive defence and military assistance, as captured here, in context of counter hybrid warfare, form the core of this study.

### **2.2.3 Special Operations Forces in CHW: NATO Perspective**

When examining NATO’s perspective on the military’s role in countering hybrid warfare tactics, it is useful to reflect upon two guiding principles that have remained constant throughout the history of democracies. First, decisions made regarding military structures and functions must not impair civilian control of the military. Second, neither structures nor functions may infringe upon the individual rights of the nation’s citizenry [18]. The laws and policies that stem from these principles apply to conventional forces as well as SOF, though not in equal measure. When assessing SOF’s role “in the modern security environment,” NATO’s Parliamentary Sub-committee on Future Security and Defence Capabilities cited aspects of NATO doctrine that capture SOF’s unique nature relative to conventional forces:

*NATO Allied Joint Doctrine for Special Operations defines SOF as the following: ‘Military activities conducted by specially designated, organised, selected, trained, and equipped forces using unconventional techniques and modes of employment’. The definition goes on to specify: “These activities may be conducted across the full range of military operations, to help achieve the desired end-state. Politico-military considerations may require clandestine or covert techniques and the acceptance of a degree of political or military risk not associated with operations by conventional forces. Special Operations deliver strategic or operational-level results or are executed where significant political risk exists” [4].*

The NATO report discusses the importance of exercising political oversight over SOF operations while maintaining adequate secrecy. Directly to considerations for SOF’s responsibilities in a hybrid environment, the report describes “Grey Zone” (aka hybrid) tactics employed by competitors in an “attempt to remain below the threshold of Article 5, which would bring to bear the overwhelming power of the Alliance into a conflict – which, at present, any opponent would lose. To parry competitors’ Grey Zone tactics, SOF can provide essential special reconnaissance, intelligence and precision operations” [4].

#### **2.2.4 NATO’s Recognition of the Counter Hybrid Warfare – Capacity Building Nexus**

NATO also explicitly recognised the relationship between counter hybrid warfare and capacity building. During the Warsaw Summit of 2016, NATO commissioned the Comprehensive Assistance Package (CAP) for Ukraine [19]. Incited by Russia’s ongoing war against its independent neighbour, the CAP was envisaged to support Ukrainian aspirations of safeguarding its territorial integrity and becoming militarily interoperable with NATO. In short, the CAP is an international agreement that defines NATO and Ukraine’s cooperative approach to capacity building. It is notably apparent that the Allies did not intend for the CAP to be a generic diplomatic implement. On the contrary, within the comprehensive defence and security reforms rubric, NATO clearly recognised that the CAP would enhance Ukraine’s ability to defend itself against hybrid warfare tactics. Along with specifying “Countering Hybrid Warfare” as one of the package’s thirteen “Support Measures”, the larger context for the CAP is plainly stated in the *Summit Communiqué*: “The Alliance is committed to effective cooperation and coordination with partners and relevant international organisations, in particular the EU, as agreed, in efforts to counter hybrid warfare.” [20]. Thus, NATO’s support to Ukraine’s defence and security reforms includes a discernible relationship between capacity building and counter hybrid warfare.

With the nexus identified between counter hybrid warfare, comprehensive defence, capacity building and special operations forces, the study now focuses on UAFSOF development. The analysis that follows concentrates on three aspects of the NATO-Ukraine project:

- 1) Legal and policy frameworks;
- 2) Unity of effort achieved through SOF’s unique approach to capability building; and
- 3) The trajectory of the programme at the time of the 24 February 2023 full-scale Russian invasion.

Within these three areas, the case study will expose implications and practices for creating counter hybrid warfare capability within the military, SOF in particular.

#### **2.2.5 Mandating Ukrainian SOF as a Counter Hybrid Actor**

The UAFSOF development project began earnestly in 2016 as a distinct element of Ukraine’s defence and security reforms. The reforms were invigorated by the Strategic Defence Bulletin (SDB) that President Petro Poroshenko released that year. Upon signing the SDB, the president pronounced his government’s commitment to remaking the Ukrainian defence apparatus: “This is a landmark program of reform of the security sector, which is doing what has not been done for 25 years” [21].

Along with the SDB, the government issued a series of laws and policies aimed at further cohering Ukrainian Armed Forces (UAF) reforms. Among the declarations within the documents, the most relevant for this study were the mandates to become fully NATO-interoperable and the order to establish democratic oversight of the armed forces [22]. The former serves as the foundation for the NSHQ’s support to UAFSOF development; the latter provides the foundation for comprehensive defence. Both declarations repeatedly appear throughout Ukraine’s national defence guidance, with the commitment to NATO interoperability being enshrined in the Constitution as of 2019 [23], [24].

Several laws and policies were especially applicable to the SOF development project. First among them is Law No. 4795, commonly referred to as “The 2016 Law on SOF” or “the SOF Law.” In July 2016, Ukraine’s diplomatic mission to NATO described the act in official policy terms: “The law has been elaborated under the NATO standards and fully meets the tasks of the Ukraine-NATO cooperation in the context of the SOF establishment. It also complies with the provisions of the Strategic Defense Bulletin.” [25] President Poroshenko further explained his government’s view of the law relative to SOF’s role in national defence, stating, “It is absolutely important in conditions of protection of Ukraine from the

aggression unleashed by the Russian Federation against us” [25]. The SOF Law was followed almost immediately by the “2016 SOF Policy.” Together, the law and policy specified the size, structures, and missions of UAF SOF, including its assigned role in resistance (i.e., comprehensive defence).

In 2021, the Ukrainian government provided further direction and resources for implementing comprehensive defence by introducing Law No 5557 and Law No 5558. Law No 5558, “On the Number of the Armed Forces of Ukraine,” authorised the establishment of a 10,000-strong Territorial Defence Force (TDF). The law also increased SOF’s authorised strength by 1,000, making it one of Europe’s largest special operations forces, with 6,500 personnel. Law No 5557, “On Territorial Defence, Resilience and Resistance,” details SOF’s responsibilities for preparing and leading designated elements of the newly formed TDF, thereby directly linking SOF and civil society. Ukraine’s Verkhovna Rada passed the laws on 16 July 2021. Two weeks later, as a demonstration of his government’s support for SOF and commitment to integrating resistance into Ukraine’s national defence plans, President Volodymyr Zelenskyy added his signature during a ceremony marking the anniversary of the nation’s newly transformed SOF. The symbolic signing, along with the president’s accompanying remarks, made UAF SOF’s counter hybrid role unassailable and the government’s commitment to establishing a special operations force capable of conducting counter hybrid warfare tasks unquestionable:

*The next and extremely important stage in the SOF development should be the implementation of the two new laws that I tabled in parliament as urgent, adopted by a constitutional majority. These are the laws on the fundamentals of national resistance and increasing the number of the Armed Forces of Ukraine. [26]*

The mandates promulgated by the SDB and other laws and policies were operationalised within the armed forces through implementation roadmaps. Each service submitted a roadmap for approval by the Commander in Chief of the Armed Forces (CINC). “SOF Strategy 2035” was the title of the SOF roadmap. The strategy contained objectives and timelines that would lead to “full operational capability” by 2035.

Per the military adage, “The plan is nothing; planning is everything,” the act of creating the legal and policy frameworks to support defence reforms was even more significant than the details written into the body of work. The collaborative process that brought members of Ukraine’s civil society, inter-ministerial officials and parliamentarians together with international supporters and advisors resulted in two critical outcomes. First, “intellectual interoperability” was established across the community of action. The task of accounting for their equities forced stakeholders to develop a practical understanding of how counter hybrid warfare, comprehensive defence, capacity building, and SOF development would intersect to affect their areas of interest. With this understanding came the ability of a diverse collection of stakeholders to debate concepts and ideas in mutually comprehensible terms. The second outcome was Ukrainian ownership. Capacity building initiatives often lack well-contemplated objectives and are commonly driven by external supporters who under-appreciate the host nation’s cultural and procedural nuances. Ukraine presents an exceptional case, not only by having established a legal and policy framework but also by having done so through a fledgling democratic process that is itself the subject of great national pride. With pride in a system also came pride in ownership. This ownership ultimately translated into a legal architecture naturally more durable than one imposed by external actors.

From an analytical perspective, one must recognise the vision, leadership and initiative demonstrated by the government of Ukraine and Ukrainian SOF. Nevertheless, few nations could develop modern, NATO-interoperable SOF without the assistance of foreign partners. Ukraine is no exception, especially given the demanding conditions under which they were conducting the reforms. Yet, external support came with the cost of the time and human capital needed to coordinate the contributions of multiple stakeholders, each presenting distinct ideas and approaches.

### **2.2.6 Ukrainian Capability Building Environment: Crowded Space**

NATO Allies began supporting Ukraine's defensive efforts immediately following Russia's 2014 invasion of Crimea and the Donbas region. Donors delivered assistance through bilateral, multilateral, and international formats, including, inter alia, NATO, the European Union, the United Nations and the Organisation for Security and Cooperation in Europe (OSCE). Countless Nongovernmental Organisations (NGOs) also supported. The Ukrainians and donors created a myriad of forums to either track accountability, synchronise advisory and material support or both. By July 2018, according to a widely circulated brief, sixty-two advisors from a multitude of nations and organisations sat permanently in Ukraine. The actual count was likely two to three times that number, as there existed neither a central mechanism to account for foreign advisors nor an official definition to determine who fell into that category. Unity of command, a long-standing military principle, was an unrealistic goal under the existing conditions. Nevertheless, key stakeholders recognised that, at a minimum, they would need to establish some semblance of unity of effort for the envisaged reforms to be realised.

In the capacity building realm, three actors were particularly noteworthy. Each created one or more coordination platforms comprising different sets of stakeholders. First, there was the Defence Reform Advisory Board (DRAB) [27]. Established in 2016, the DRAB quickly expanded from four to six retired senior defence officials from Canada, Germany, Great Britain, Lithuania, Poland, and the United States, respectively. The board was responsible for advising the Ukrainian Minister of Defence (MOD) and other key government officials on approaches to achieving the defence and security reforms specified by the SDB. Functionally, five members of the DRAB each assumed responsibility for one of the five SDB pillars (i.e., command and control, professional military education, etc.). The sixth member was responsible for fusing developments from the five functional areas into a cohesive national defence capability. In addition to DRAB members having direct access to the defence minister, Ukraine's Defence Reforms Committee provided a natural forum through which the DRAB could coordinate. The Minister of Defence chaired the committee, which included key officials from across the government. Theoretically, the Reform Committee's membership made it the ideal body for deconflicting and synchronising initiatives. In practice, however, the ideal state was never reached due largely to the lack of a lever to compel representatives of various organisations to cooperate.

A second prominent coordinating body was the Multinational Joint Commission (MJC). The U.S. European Command's Strategy Director (J5) and a counterpart from the General Staff of the Ukrainian Armed Forces jointly chaired the MJC. Canada, Great Britain, and Lithuania were early members of the MJC, though, by 2021, it had expanded to include over a dozen participating nations. The MJC's function was to assess and prioritise training, equipment and advisory support delivered by its members to Ukraine. Its sub-committees would convene quarterly to synchronise across their thirteen functional areas, including SOF. The sub-committees reported to the executive board semi-annually. In its later years, the MJC established a standing Multinational Coordination Centre (MCC) in Kyiv to further enhance coherence. By all accounts, the MJC added value within the crowded security assistance space. However, by charter, it focused on training and equipping at the tactical level (brigade and below), rather than creating sustainable capability. For advice and assistance with the development of enduring institutional capacity, the defence and security community looked mainly toward NATO, the most prominent of the three actors.

The structures and processes NATO used to manage Alliance support to Ukrainian defence reforms were by far the most mature among all players. Ukraine joined NATO's Partnership for Peace framework in 1994 [28]; [29]. Three years later, the two parties signed a "Charter on a Distinctive Partnership between the North Atlantic Treaty Organization and Ukraine" [30]. Through the Charter, NATO and Ukraine agreed to explore opportunities to cooperate in all imaginable security areas, ranging from civil-military relations to nuclear proliferation to interoperability. The Charter also called for the establishment of the NATO-Ukraine Commission (NUC) as a "forum for consultation between the Allies and Ukraine on security issues of common concern..." [31]. During the subsequent years, NATO and Ukraine created several staffing and

coordinating bodies to manage what had “developed into one of the most substantial of NATO’s partnerships” [32]. Within Ukraine, NATO established the NATO Representation to Ukraine (NRU), which comprised the NATO Information and Documentation Centre (NIDC) and the NATO Liaison Office (NLO). The subject matter experts assigned to the NLO, including political and military advisors, were responsible for managing NATO-Ukraine defence reform cooperation [32], [33]. The head of the NLO held ambassadorial-level diplomatic status and corresponding access to Ukrainian government officials. In addition to the various coordination forums it convened, the NRU enjoyed admission to forums hosted by the other actors as either observers or active participants. In this sense, the NRU served as a seam connector and clearinghouse.

In practice, personnel shortages and a lack of formal coordinating authority often hampered the NRU’s effectiveness as a cross-functional coordinator. The majority of the NRU staff was Ukrainian, with responsibilities ranging from administration, logistics and physical security to strategic communications and political analysis. They proved invaluable, and their positions were seldom vacant. Core NATO staff posts, on the other hand, were filled primarily through a Voluntary National Contribution (VNC) system. As the name implies, VNCs are personnel nations voluntarily provide to fill positions outside permanent Alliance structures. Assigned personnel must meet NATO-specified qualifications, though shortages often lead to compromise, and positions often go unfilled for extended periods.

The bodies that formed to coordinate bilateral, multilateral and Alliance support to Ukraine’s defence and security reforms all sought to reduce confusion and redundancy among the innumerable stakeholders operating within an extremely crowded space. Nevertheless, each coordinating entity had limitations, and the whole never became greater than the sum of its parts. Analysis reveals that one of the greatest challenges to achieving a truly unified effort was a reluctance on the part of several influential nations to deliver their contributions through NATO Partnership modalities, despite the relative ease of doing so. Nearly all nations providing support bilaterally were members of the Alliance. Thus, they had approved NATO to deliver that same support, only to hamper the Alliance’s ability produce results. This phenomenon defines the space and conditions under which Alliance SOF conducted military assistance to bolster Ukrainian counter hybrid warfare capability.

### **2.2.7 SOF Unity of Command**

Having established a coordination centre charged with creating common standards and doctrine for Alliance SOF and having served shoulder to shoulder through multiple tours in Afghanistan, by 2016, the SOF of the Alliance had evolved into a tightly knit network.<sup>4</sup> Relationships and common approaches greatly enhanced their ability to navigate the crowded space that defined the Ukrainian capability building environment. Still, even SOF needed help to avoid the redundancy and waste that stemmed from the multitude of ad hoc approaches being applied in support of reforms. Through four measures, implemented iteratively and often in response to failures, SOF achieved unity of effort:

- 1) Formed disparate Allied elements into a recognisable, albeit informal, unit of action,
- 2) Integrated the unit into the Ukrainian defence reform ecosystem,
- 3) Created a single plan to guide UAFSOF development, and
- 4) Established a common approach to capacity building, or in SOF parlance, military assistance.

As an initial step, SOF representatives from nine nations assembled at the NSHQ in Mons, Belgium in November 2017 to conduct the first of what became a continuing series of Ukrainian “SOF Development Workshops.” Each attending nation either regularly contributed to Ukrainian SOF development or intended

---

<sup>4</sup> The NATO Special Operations Coordination Centre (NSCC) was established in 2008. In 2012, it was re-designated as the NATO Special Operations Headquarters. As this study was being conducted, it was undergoing another transformational modernisation, to include a retitling as Alliance Special Operations Forces Command.



to do so in the future. In most cases, nations provided their contributions through bilateral arrangements, with the MJC accounting for some and NATO tracking very few. The assembled group accomplished their two planned goals, along with a third unintended achievement. First, they aligned the timing and purposes of their bilateral contributions to best support mutually agreed objectives. Second, they drafted recommended updates to the portions of framework NATO-Ukraine partnership documents deemed relevant to SOF development. The aim was to align bilateral capability development activity with Ukraine's "Partnership Goals." Third, to ensure this close collaboration would continue, participants agreed to form themselves into an informal body, which they named the "Multinational SOF Advisory Team (MSAT)." The group developed four rules to govern the MSAT and later presented the terms to Allied SOF commanders for their approval:

- 1) To the greatest extent possible, ensure all bilateral contributions will align with the SOF Development Plan;
- 2) To the greatest extent possible, each MSAT member nation allows other MSAT members to observe or participate in its events. This would reduce redundancy among Allies, and facilitate the dissemination of best practices, thus reinforcing common standards;
- 3) Ensure any bilateral activities that must occur outside of the MSAT framework do not interfere with the plan; and
- 4) Do not share information that a team member may inadvertently discover about bilateral plans and activities outside the MSAT framework.

As the MSAT was forming and evolving, it was also refining the SOF Development Plan so all could agree and cooperatively implement it. The most critical stakeholder in this endeavour was Ukrainian SOCOM. Thus, the team deliberately transitioned oversight of the coordination process to its Ukrainian counterparts. In February 2018, the MSAT reconvened at Ukrainian SOCOM headquarters, where the group again reviewed the development plan and supporting contributions, this time with direct Ukrainian guidance and input. The stakeholders continued to refine and expand their cooperative approach. By February 2022, the MSAT had grown from nine member nations to seventeen. MSAT coordination comprised weekly meetings for in-country advisors, chaired by Ukrainian SOCOM; monthly meetings, also led by Ukrainian SOCOM and supported by NSHQ; quarterly updates to Allied SOF commanders, who were commonly referred to as the "MSAT commanders;" and biannual SOF Development Workshops, where plans would be collaboratively assessed and updated against a three-year horizon. Stakeholders outside of SOF also participated in the biannual workshops; i.e., representatives from the Navy, Air Force, Air Assault, General Staff, Border Guard Services, etc. Critically, the MSAT's planning and coordination process allowed SOF to more effectively engage the myriad of other guiding and coordination activities occurring within the defence and security reform space, such as the NATO Partnership Planning and Review Process, numerous forums associated with the Comprehensive Assistance Package, the U.S. frame-worked MJC and Ukraine's own Annual National Plan, among others.

Through cohering plans and processes in support of Ukrainian SOF development, the SOF advisory network naturally became more coherent as well. Several nations provided in-country SOF advisors to Ukrainian SOCOM headquarters and nearly all of its regiments.<sup>5</sup> The group considered one among them to be the "Senior SOF Advisor," and two of similar seniority were formally dual-hatted to represent their respective nations as well as the NSHQ. In their capacity as "NSHQ Points of Presence", they were also members of the NATO Liaison Office advisory team. One of the points of presence sat in the MJC's MCC in Kyiv, and both regularly interfaced with their respective nation's DRAB representative. Both were also members of the MJC's SOF subcommittee, which the Senior SOF Advisor chaired. Finally, the NSHQ provided a retired SOF general officer as the Strategic SOF Advisor (SSA). The SSA position was formally agreed upon through an exchange of letters between NATO's Assistant Secretary General for Operations and the First Deputy Secretary of the National Security and Defence Council of Ukraine in their capacities as co-chairs of

---

<sup>5</sup> Ukraine also refers to its SOF regiments as centres for doctrinal reasons.

the NATO-Ukraine Joint Working Group on Defence Reform, a NUC subcommittee. All Allies also reviewed and endorsed the agreement in accordance with NATO's silence procedures. The SSA was responsible for advising senior Ukrainian civilian and military officials on the integration of NATO-interoperable SOF capabilities into the national defence and security apparatus [34]; [35]. Although not permanently on site, the SSA was member of the NRU team operating under the NSHQ's direct guidance. Responsibility for synchronising the MSAT advisors in terms of NATO-Ukraine objectives fell to the NSHQ Partnership Directorate (J9).

By applying this network approach, the MSAT deliberately integrated itself into the Ukrainian defence and security reform ecosystem. In particular, in some capacity, SOF personnel were formally associated with each of the three critical nodes: MJC, DRAB, and NRU. Consequently, the MSAT was able to ensure that all members were continuously aware of the potential impacts various reform initiatives would have on their planned investments. With this information, all stakeholders could adjust accordingly. Equally important, SOF's positioning enabled it to inform the direction of the reforms by rendering advice where appropriate, without exceeding the bounds of its mandate.

The fourth element of the MSAT's unity of effort was a common capacity building approach. Among Allied SOF, the paradigm for military assistance was born largely from SOF's experiences in Afghanistan. SOF conducted capability building activities in Iraq and across the African continent in similar fashion. Allied tactical organisations paired with, trained, and in some cases accompanied their partner units into combat. The Ukrainian situation differed greatly from the MA model with which the Allies had become accustomed. Rather than simply training tactical units, Allied subject matter experts were called upon to advise and assist with integrating SOF capabilities into the fabric of Ukrainian defence institutions. Prior to forming the MSAT, bilateral support focused principally on tending to UAFSOF's "immediate needs." They accomplished this by deploying mobile training teams, affording access to national and NATO training courses and conducting joint exercises. Allies provided a "train the trainer" programme at the more advanced level to lead to UAFSOF self-sufficiency.

As Ukraine and NATO increased focus on defence reforms, SOF's traditional MA methods proved inadequate for creating enduring capability. Thus, the group developed a new approach, initially dubbed "Advanced MA." Advanced MA was grounded by the notions of "building the factory" and "we (Allied SOF) do not support training; we support development." According to the idea of building the factory, training UAFSOF operators and even "train the trainer" programmes were analogous to producing a product. For UAFSOF to become self-sufficient, they would need to be able to produce their own products. This was true not only of training themselves but of every capability. The SOF Development Plan reflected the factory-building approach, which revolved around a set of "capability packages." Per NATO's definition, to be complete, a capability must include Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability (DOTMLPFI). Regarding supporting development vice training, stakeholders, including UAFSOF, agreed to link all activities to create a measurable capability. In the MSAT's colloquial terms, there would be no "random acts of touching," or "RATS." This further reinforced the role of the SOF Development Plan with its DOTMLPFI construct.

Using the new model, UAFSOF and their Allied counterparts began to create "math problems." For example, based on the structure mandated in law and policy, they would require a certain number of SOF medics. The medics would need to be trained according to NATO norms and standards. This was a relatively simple matter of calculating the number of instructors needed to train the required number of medics. Less intuitive, the teams would also have to calculate retention rates; i.e., how many medics would be promoted out of certain positions or leave the service each year? The calculations, yield both the initial surge and enduring sustainment requirements. This first step fell mostly into the category of "P" in DOTMLPFI. Other steps included determining what doctrine was required and how that would be produced and sustained, implications for organisational structure – how medics would be distributed, to include instructor cadres and systems to qualify instructors, etc. In this example, in particular, even legal implications had to be

considered. Like many European nations, laws governing medical certifications needed to be modified to account for the advanced level of training SOF medics require. Detailed analysis continued until each portion of the plan included all requirements for materiel, facilities, and so forth. The MSAT would then continually scrutinise the plan to identify how each element would affect others. In addition, the plan identified the approving authority for each step. If a policy or legislative action was required, the approving authority could be the president or the Rada.

Consequently, UAFSOF rapidly assumed more responsibility for designing and conducting ongoing training. At the same time, the collective's emphasis shifted from courses and exercises to tailored workshops where participants would build standing operating procedures, equipment requirement lists that included sustainment costs, recommended legislative language and so on. The MSAT would then package the results to guide prioritised, incremental capability development; e.g., the capability to train SOF medics without Allied support. Thus, a capability package was akin to an individual Lego that the team could create in two to three years and later snap together with other packages to form the fully operationally capable special operations force specified in "UAFSOF Strategy 2035." On 24 February 2022, six capability packages were under construction.

### **2.2.8 Forward Trajectory**

The last Ukrainian MSAT workshop convened in October 2021. The next had been confirmed for February 2022, just before Russia's full-scale invasion. Stakeholders decided to postpone the February workshop due to heightening tensions. However, the team's intentions reveal a positive glide slope for the programme and the process that supported it. Per the norm, the MSAT had planned to use the workshop to formally assess the progress of the six capability packages and conduct general coordination. The team also intended to propose changing the title of those supporting Ukrainian development from "advisor" to "integrator." The prospective change was both a sign of respect and an acknowledgement of progress. UAFSOF no longer required the type of "coaching, teaching and mentoring" they had needed at the start of the reforms. By this time, partners of equal status were developing solutions for integrating NATO-interoperable capabilities. For example, the NSHQ J9 had relied heavily on UAFSOF advice as they created the *Comprehensive Defence Handbook*, the *Building SOF Capability Handbook*, and the "How to Build SOF" course for the NATO Special Operations University.

Development support did not end with the full-scale invasion. Per the direction the Heads of State and Government delivered at NATO's 2022 Madrid Summit, the Alliance conducted an "extraordinary review of the CAP" to identify support to be rendered under the new conditions. SOF's relationship with UAFSOF continues via NSHQ and bilaterally, in support of revised CAP objectives.

The NATO-Ukraine SOF development project also positively influenced NATO's approach to capacity building. MSATs now exist for all NATO Partners whose SOF receive capacity building support from the NSHQ. Also, within the framework of NATO 2030, Supreme Headquarters Allied Powers Europe (SHAPE) is creating a capacity building organisation based largely on NSHQ's approach [36].

## **2.3 DEDUCTIONS AND CONCLUSIONS**

Hybrid warfare, comprehensive defence and capability building are accepted terms of art among military and foreign affairs professionals. However, none of the terms is authoritatively defined or universally accepted. Moreover, each is normally contemplated separately from the others. Exceptionally, this case study of Ukrainian SOF development reveals the counterintuitive nexus between the three paradigms and SOF. Within this multi-dimensional construct, it is possible to recognise SOF's role in capacity building as a counter hybrid warfare action. Moreover, the action compounds itself insofar as its purpose is to produce a counter hybrid capability. More specifically, from this brief investigation, five deductions are most readily apparent:

- 1) Updated Ukrainian legal and policy frameworks provided clear, measurable objectives that proved vital to establishing a coherent approach to capability development;
- 2) NATO and Ukraine Partnership agreements enabled Allies to align international advice and assistance with Ukrainian-approved objectives;
- 3) Establishing a recognisable unit of action, in this instance, the MSAT, and a mutually agreed SOF Development Plan, enabled Allied SOF to align bilateral contributions with Ukraine's SOF development objectives easily;
- 4) Integrating the unit of action into the Ukrainian defence reform ecosystem allowed all MSAT members to make sound investment decisions and responsible defence reform advice; and
- 5) Allied SOF's traditional methods for conducting MA, which were grounded in force generation approaches, proved inadequate for supporting the creation of enduring capability and, therefore, transitioned to a more comprehensive Force Development-based MA model.

These deductions are specific to the context of Ukrainian defence and security reforms and SOF's role in capacity building between 2017 and 2022, prior to Russia's full-scale invasion. However, the lessons associated with the deductions are not necessarily limited to SOF or the Ukrainian case. When building capacity, the benefits of assigning clear, measurable objectives, establishing a recognisable unit of action, and so on, apply equally to conventional forces and even nongovernmental organisations as to SOF. Indeed, though more limited in function than the MSAT, the MJC was a recognisable unit of action responsible for aligning bilateral contributions. Likewise, SOF was a relatively minor component within the Comprehensive Assistance Package for Ukraine and other formal Partnership agreements. The notable, often intangible, difference seems to lie in SOF's ability to integrate seamlessly into their environment and a proclivity to leverage existing mechanisms beyond their envisioned capacity and purpose while remaining within the bounds of relevant policy. These abilities and tendencies are partly the inherent nature of SOF, as described in the NATO parliamentary study. They are also partly a consequence of the deliberately formed Global SOF Network, as demonstrated through the MSAT.

## **2.4 REFERENCES**

- [1] Atlamazoglou, S. "Ukrainian Special-Operations Forces Doubled in Size while Training with the US, Top US Special-Ops Commander Says." Business Insider, 10 June 2022.
- [2] Yoho, K.D., Deblanc-Knowles, T. Borum, R. et al. "The Global SOF Network: Special Issue Summer 2014." Journal of Strategic Security, 7(2), 2014. <https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1380&context=jss>
- [3] Szayna, T.S., and Welser IV, W. "Developing and Assessing Options for the Global SOF Network." RAND Corporation, 2013. [https://www.rand.org/pubs/research\\_reports/RR340.html](https://www.rand.org/pubs/research_reports/RR340.html)
- [4] NATO Parliamentary Assembly. Defence and Security Committee (DSC) Sub-Committee on Future Security and Defence Capabilities (DSCFC). "NATO Special Operations Forces in the Modern Security Environment." 69 DSCFC 18 E rev.1 fin, 2018. <https://www.nato-pa.int/download-file?filename=/sites/default/files/2018-12/2018%20-%20SPECIAL%20OPERATIONS%20FORCES%20-%20MOON%20REPORT%20-%20169%20DSCFC%2018%20E%20rev.1%20fin.pdf>
- [5] Allied Command Transformation, ACT. NATO and Partners Build Capacity Infrastructure. 13 July 2022. Available at: <https://www.act.nato.int/article/nato-and-partners-build-capacity-infrastructure/>
- [6] NATO Special Operations Headquarters, NSHQ. Official Website. Allied Special Operations Forces Command (SOFCOM), 2023. [www.nshq.nato.int](http://www.nshq.nato.int)

- [7] Solmaz, T. “Hybrid Warfare: One Term, Many Meanings.” *Small Wars Journal*, 2022. <https://smallwarsjournal.com/jrnl/art/hybrid-warfare-one-term-many-meanings>
- [8] Dowse, A., and Bachmann, S.-D. “Explainer: What is ‘Hybrid Warfare’ and What is Meant by the ‘Grey Zone’?” *The Conversation*. 17 June 2019. <https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841>
- [9] Whither, J. “Making Sense of Hybrid Warfare.” *Connections*, 24, 2016.
- [10] NATO Special Operations Headquarters, NSHQ. *Comprehensive Defence Handbook, Vol I. Edition A Version 1 December 2020*. NATO Special Operations Headquarters, Belgium, 2020a.
- [11] NATO Special Operations Headquarters, NSHQ. (2020b). *Comprehensive Defence Handbook, Vol I. Edition A Version 1 December 2020*. NATO Special Operations Headquarters, Belgium, 2020b
- [12] Naval Postgraduate School. *Special Operations/Irregular Warfare Curriculum 699, 2023b*. Available at: <https://nps.smartcatalogiq.com/en/current/academic-catalog/departments/department-of-defense-analysis/special-operations-irregular-warfare-curriculum-699/>
- [13] Naval Postgraduate School. *International Programs Catalog 2023-2024*. 2023a. <https://nps.edu/documents/103449453/0/2023-2024+NPS+IGPO+Catalog+-+Final+%281%29.pdf/cb30788b-a1e8-53b8-9494-c74aab79dd75?t=1675466722992>
- [14] Freeman, M., Simons, A., Skinner, E. (eds.) (2016). *Special Issue: Countering Hybrid Warfare: The Best Uses of SOF in a Pre-Article V Scenario*. *Combatting Terrorism Exchange (CTX) Journal*, 6(4). <https://core.ac.uk/download/pdf/81223163.pdf>
- [15] Webb, Marshall B., Lt Gen. “Foreword.” *Special Issue: Countering Hybrid Warfare: The Best Uses of SOF in a Pre-Article V Scenario*. *Combatting Terrorism Exchange (CTX) Journal*, 6(4), 2016, pp.5-6. <https://core.ac.uk/download/pdf/81223163.pdf>
- [16] Berg-Knutson, E. “From Tactical Champions to Grand Strategy Enablers: The Future of Small-Nation SOF in Counter-Hybrid Warfare.” *Special Issue: Countering Hybrid Warfare: The Best Uses of SOF in a Pre-Article V Scenario*. *Combatting Terrorism Exchange (CTX) Journal*, 6(4), pp. 61-68, 2016. <https://core.ac.uk/download/pdf/81223163.pdf>
- [17] Kristiansen, M., and Hedenstrøm, A. “NATO SOF Military Assistance to Support Deterrence and Reassure Russia.” *Special Issue: Countering Hybrid Warfare: The Best Uses of SOF in a Pre-Article V Scenario*. *Combatting Terrorism Exchange (CTX) Journal*, 6(4), 2016, pp. 90-99. <https://core.ac.uk/download/pdf/81223163.pdf>
- [18] Huntington, S.P. *The Soldier and the State: The Theory and Politics of Civil-Military Relations*. Harvard University Press. Cambridge, MA, 1957.
- [19] North Atlantic Treaty Organization. “Comprehensive Assistance Package for Ukraine.” *Fact Sheet*. July 2016b. [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/pdf\\_2016\\_09/20160920\\_160920-compreh-ass-package-ukraine-en.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_09/20160920_160920-compreh-ass-package-ukraine-en.pdf)
- [20] NATO Heads of State and Government. *Warsaw Summit Communiqué*. 09 July 2016. Par. 72, [https://www.nato.int/cps/en/natohq/official\\_texts\\_133169.htm#hybrid](https://www.nato.int/cps/en/natohq/official_texts_133169.htm#hybrid)

- [21] Interfax-Ukraine. “Poroshenko enacts Ukraine’s Strategic Defense Bulletin.” Kyiv Post. 27 May 2016. <https://archive.kyivpost.com/article/content/ukraine-politics/poroshenko-enacts-ukraines-strategic-defense-bulletin-414836.html>
- [22] Sanders, D. “Ukraine’s Third Wave of Military Reform 2016 – 2022 – Building a Military Able to Defend Ukraine Against the Russian Invasion.” Defense & Security Analysis, 2023. DOI: 10.1080/14751798.2023.2201017
- [23] Radio Free Europe. “Ukraine President Signs Constitutional Amendment On NATO, EU Membership.” 19 February 2019. <https://www.rferl.org/a/ukraine-president-signs-constitutional-amendment-on-nato-eu-membership/29779430.html>
- [24] Verkhovna Rada of Ukraine. Constitution of Ukraine Adopted at the Fifth Session of the Verkhovna Rada of Ukraine on June 28, 1996. No. 2680-VIII, dated February 7, 2019. [https://ccu.gov.ua/sites/default/files/constitution\\_2019\\_eng.pdf](https://ccu.gov.ua/sites/default/files/constitution_2019_eng.pdf)
- [25] Mission of Ukraine to the North Atlantic Treaty Organization. “President Signed Law on AFU Special Operations Forces.” 27 July 2016. <https://nato.mfa.gov.ua/en/news/49519-president-pidpisav-zakon-shhodo-sil-specialnyih-operacij-zsu>
- [26] Chaharnyi, O. “Zelensky Increases Number of Armed Forces, Signs Laws on National Resistance.” Kyiv Post, 29 July 2021. <https://archive.kyivpost.com/ukraine-politics/zelensky-increases-the-number-of-the-armed-forces-signs-laws-on-national-resistance.html>
- [27] Rahemtulla, R. “Ukraine Relies on Advice from Defense Reform Advisory Board.” Kyiv Post, 17 November 2016. <https://www.kyivpost.com/post/8936>
- [28] North Atlantic Treaty Organization, NATO. Signatures of Partnership for Peace Framework Document, 27 March 2020. [https://www.nato.int/cps/en/natolive/topics\\_82584.htm](https://www.nato.int/cps/en/natolive/topics_82584.htm)
- [29] North Atlantic Treaty Organization, NATO. (2023a). Partnership for Peace Programme, 11 April 2023. [https://www.nato.int/cps/en/natohq/topics\\_50349.htm](https://www.nato.int/cps/en/natohq/topics_50349.htm)
- [30] North Atlantic Treaty Organization, NATO. Charter on a Distinctive Partnership between the North Atlantic Treaty Organization and Ukraine. 09 July 1997. [https://www.nato.int/cps/en/natohq/official\\_texts\\_25457.htm](https://www.nato.int/cps/en/natohq/official_texts_25457.htm)
- [31] North Atlantic Treaty Organization, NATO. (2023c). “NATO-Ukraine Commission (1997 – 2023).” 13 July 2023. [https://www.nato.int/cps/en/natohq/topics\\_50319.htm](https://www.nato.int/cps/en/natohq/topics_50319.htm)
- [32] North Atlantic Treaty Organization, NATO. (2023b). “Relations with Ukraine.” [https://www.nato.int/cps/en/natohq/topics\\_37750.htm](https://www.nato.int/cps/en/natohq/topics_37750.htm)
- [33] North Atlantic Treaty Organization, NATO. (2006). “NATO Military Liaison Office in Kyiv.” 21 September 2006. [https://www.nato.int/structur/nmlo/nmlo\\_kyiv.htm](https://www.nato.int/structur/nmlo/nmlo_kyiv.htm)
- [34] General Staff of the Armed Forces of Ukraine (2021). “Commander-in-Chief Zaluzhny Meets with Adviser of NATO Representation to Ukraine.” Ukrinform, 12 August 2021. <https://www.ukrinform.net/rubric-defense/3296443-commanderinchief-zaluzhny-meets-with-adviser-of-nato-representation-to-ukraine.html>

- [35] Presidential Office of Ukraine. “Deputy Head of the President’s Office Roman Mashovets Discussed Prospects for Defense Cooperation with NATO Strategic Advisor on SOF Issues.” 24 June 2021. <https://www.president.gov.ua/en/news/zastupnik-kerivnika-ofisu-prezidenta-roman-mashovec-obgovori-69213>
- [36] North Atlantic Treaty Organization, NATO. “NATO 2030.” Fact Sheet, June 2021. [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf)





## Chapter 3 – ORGANIZATION OF TERRITORIAL DEFENCE OF UKRAINE UNDER THE HYBRID WAR WITH RUSSIA

V.S. Frolov and V.M. Semenko<sup>1</sup>  
National Defence University of Ukraine  
UKRAINE

### 3.1 INTRODUCTION

With the possibility of an invasion by the Armed Forces of Russia, the question of Ukrainian territorial defence against hybrid threats remains acute. The aggressive essence of contemporary Russian policy and how this manifests itself in hybrid measures is reflected in the four main directions [Ed.: vectors] of threat to Ukrainian national interests described in this chapter. The organization of the territorial defence system is an insufficiently studied element of the organization of the defence of Ukraine. This chapter goes on to outline the main problems with the organization of the territorial defence system in Ukraine, relevant foreign experiences, areas for improvement and a variant of the structure of the territorial defence of Ukraine. The relevance of this chapter is confirmed by the Law “On the Fundamentals of National Resistance” which entered into force on 1 August 2021 and comes into force on 1 January 2022.

The beginning of the 21<sup>st</sup> century has been characterized by the intensification of the imperial ambitions of the Russian Federation (RF). Its national interests have deep historical roots, which originated in the early days of the formation of “Muscovy”, then developed during the Russian Empire and the Soviet Union. In a relatively short period of time, Kremlin leaders managed to build a form of imperialism in post-Soviet Russia, which is essentially modeled on the ideologues of communism: the unlimited power of capital, the ruthless exploitation of the working class, the militarization of the economy and the arms race, and world domination, etc.

To restore the empire, the Russian Federation chose the most dangerous and aggressive way available – direct military aggression against the states of the former USSR and the occupation of part of their territories. The main purpose of such actions is to forcibly bring the peoples of these states under Russian jurisdiction. The creation of the “Transnistrian Republic”, the capture of Abkhazia and South Ossetia, the occupation of Crimea and eastern Ukraine confirm the Kremlin’s imperial ambitions. The Russian Federation has launched military operations in Syria in order to prevent the Middle East’s energy resources from entering the European market to the detriment of Gazprom and to declare to the world community its ambitions in the geopolitical space as one of the world leaders.

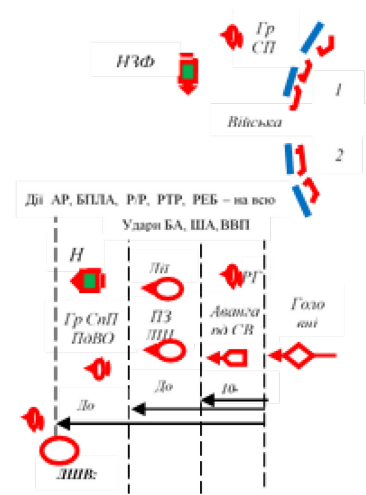
In our opinion, the modern policy of the Kremlin government of the Russian Empire of the 21st century is based on:

- Neo-fascist ideology of the “Russian world”;
- The most aggressive features of foreign policy of the 19<sup>th</sup> – 20th centuries; and
- Stalin’s repressive system of public administration.

The preparation and conduct of a hybrid war against Ukraine reflects the real essence of Russia’s current aggressive policy. The main directions of threats to the national interests of Ukraine by the Russian Federation in the conditions of hybrid warfare, analyzed by the authors in a previous article [1], are shown in Figure 3-1.

---

<sup>1</sup> **Note from SAS-161 RTG Co-Chair Neil Chuka:** This chapter is a modified and translated adaptation of an article originally published by the authors in the Ukrainian academic journal Science and Defence, 2, 2021. The positions of Mr. Frolov and Col. Semenko are noted as they were at the time this chapter was first produced in late 2021.

	<b>The First Direction</b>	<b>The Second Direction</b>	<b>The Third Direction</b>	<b>The Fourth Direction</b>
<b>Effects</b>	<p><b>“Soft” War</b></p> <p>Use of the UN, OSCE and other organizations to discriminate against Ukraine;</p> <p>Use of financial, economic and energy leverages against Ukraine;</p> <p>Blocking Ukraine’s cooperation with the EU and NATO;</p> <p>Application of diplomatic measures, etc.</p>	<p><b>Information Struggle</b></p> <p>Organization of information warfare in order to: discredit the authorities of Ukraine;</p> <p>Formation of pro-Russian views among the population;</p> <p>Strengthening anti-Ukrainian sentiment in Russia;</p> <p>Activation of systemic cyberattacks, etc.</p>	<p><b>Interference in Internal Affairs</b></p> <p>Destabilization of the domestic political situation:</p> <p>Intensification of anti-state political forces;</p> <p>Linking criminal elements;</p> <p>Formation of NPF;</p> <p>Sabotage in arsenals, warehouses, rallies, protests and blocking of government work, etc.</p>	<p><b>Military Action (Provided that the population supports aggression)</b></p>  <p>ПДВО – Southern Military District of the RF;</p> <p>НЗФ- Illegal armed groups.</p>
<b>Means</b>	<ol style="list-style-type: none"> <li>1) State Duma</li> <li>2) President of the Russian Federation</li> <li>3) Council of Ministers of the Russian Federation</li> <li>4) Diplomatic Corps RF</li> </ol>	<ol style="list-style-type: none"> <li>1) State Duma</li> <li>2) President of the Russian Federation</li> <li>3) FSB; MO; GRU GS RF; CO forces</li> <li>4) Pro-Russian political parties</li> </ol>	<ol style="list-style-type: none"> <li>1) President of the Russian Federation</li> <li>2) FSB; GUR GS; Private Mil Comp</li> <li>3) Cossacks military formation of the RF</li> <li>4) RG of the Southern Military District of the RF</li> </ol>	
	5) Foreign intelligence of the Russian Federation			

**Figure 3-1: Elements of the Hybrid War of the Russian Federation Against Ukraine.**

In preparing and conducting a hybrid war against Georgia and Ukraine, the Russian Federation uses the latest methods of applying pressure on national interests *in four main directions*:

**The first direction:** *Use of soft power measures to discriminate against Ukraine in areas of international cooperation such as economics, logistics, and energy supplies.* Diplomatic affairs are similarly discriminatory with violations of both international law and treaties of bilateral relations. Russia’s so-called “soft” war against Ukraine and other post-Soviet republics has not stopped since the collapse of the former USSR.

**The second direction:** *Deploying and conducting aggressive information and cyber warfare.* A. Illarionov, a researcher at the Cato Institute (Washington, USA) and former adviser to Vladimir Putin, considers the modern information struggle to be the Fourth World War and states:

*The information war is the first total world war. Both in the First World War, and in the Second World War, and in the so-called Third World (Cold) Wars, theaters of war, fronts, flanks, and rear were clearly delineated. ... Due to its immanent qualities, information has the property of spreading, despite borders and certain limitations. Therefore, the information war has no rear or flanks. The fronts of information warfare can run anywhere [2].*

The information war is being constantly waged by the Russian Federation in the geopolitical space and covers all spheres of activity. It is carried out regardless of the level and condition of relations between states (or groups of states). The main purpose of RF information operations is to spread and protect the nationalist ideas of the “Russian world”, to justify military aggression against neighboring states and the use of armed groups on other continents [3].

**The third direction:** *Interference in the internal affairs of state bodies.* The Russian Federation actively uses a set of asymmetric means to destabilize the domestic political situation of rival states. Using the results of the first and second directions of threats to national interests, the Russian Federation tries to complicate the activities of government structures within rival states by negatively affecting social, economic and other domestic processes and activities. At the global level this is characterized by interfering in elections, support for movements and political parties with extremist views or amenable to RF perspectives, and by embedding military or other RF government agents or proxies into terrorist organizations.

In the post-Soviet countries Russia’s interference in internal affairs is both greater and more comprehensive:

- Formation and financial support of political parties, separatist movements and pro-Russian media;
- Comprehensive support of pro-Russian candidates for elections (appointments) to public authorities;
- Conducting comprehensive measures to discredit the political leadership of states; and
- Formation of a reconnaissance network in enemy territory and escalation of the criminal behaviors meant to undermine state authority.

**The fourth direction:** *Military aggression.* Armed aggression is usually a forceful continuation of the foreign policy goal not achieved by the use of “soft war” – the forces, means and methods of the previous three directions. One of the main conditions for the invasion of RF Armed Forces (AF) into the territory of neighboring states is the tacit or explicit support of a large number of local people. In other words, a major RF planning assumption is that the arrival of RF Armed Forces would be welcomed by some portion of the local population. The lack of such support complicates the justification of any occupation in terms of international law, complicates the possibility of forming local governments that would act in the interests of the aggressor state, and requires significant emergency measures to maintain the occupation regime in the occupied territories. The analysis of the population’s support from the beginning of the aggression to the present day in the threatened regions of Ukraine is given in the research of the National Institute for Strategic Studies “Ukrainian Frontier” [4], [5], [6].

### 3.2 LEVELS OF RF HYBRID AGGRESSION

Planning, organization, support and management of Russia’s hybrid military aggression against Ukraine can be divided into *four levels* as shown in Table 3-1.

**Table 3-1: The Sequence of the Main Measures of the Russian Hybrid Aggression Against Ukraine.**

Organization and Management	Performers	The Main Measures of “Hybrid” Aggression
<b>1) Formation of the plan of “hybrid” aggression of the Russian Federation against Ukraine</b>		
Political leadership of the Russian Federation, FSB, MD.	<ol style="list-style-type: none"> <li>1) General Staff of the Armed Forces.</li> <li>2) FSB departments.</li> <li>3) Headquarters of military districts, navies, VAT, types of the ZS of the RF.</li> </ol>	<ol style="list-style-type: none"> <li>1) Determining the political purpose of aggression.</li> <li>2) Development of plans of operations, methods and methods of their implementation.</li> <li>3) Organization of comprehensive support.</li> </ol>
<b>2. Political platform of “hybrid” aggression of the Russian Federation in Ukraine</b>		
<ol style="list-style-type: none"> <li>1) The Party of Regions and its allies.</li> <li>2) Communist Party of Ukraine.</li> <li>3) Russian political parties in the ARC.</li> </ol>	<ol style="list-style-type: none"> <li>1) Pro-Russian part of the population.</li> <li>2) Pensioners and the population of “Soviet” orientation.</li> <li>3) Representatives of the criminal business.</li> <li>4) Deserters of the Ministry of Internal Affairs, the Armed Forces, the Security Service, the Prosecutor’s Office, and the courts.</li> </ol>	<ol style="list-style-type: none"> <li>1) Formation of occupation authorities.</li> <li>2) Organization of administrative management in the annexed territories.</li> <li>3) Persecution of patriotic forces under the guise of bringing order.</li> <li>4) Information and propaganda anti-Ukrainian activity.</li> <li>5) Organization of rallies in support of the “Russian Spring”.</li> </ol>
<b>3. The use of the Armed Forces and other military formations of the Russian Federation in “hybrid” aggression</b>		
<ol style="list-style-type: none"> <li>1) Operational groups of the General Staff of the Armed Forces, VAT and the FSB of the Russian Federation.</li> <li>2) Command of the Southern Military District and the Black Sea Fleet of the RF.</li> </ol>	<ol style="list-style-type: none"> <li>1) Agency of the GRU GS, FSB of the Russian Federation in Ukraine.</li> <li>2) VAT SPP groups, GRU ZS and FSB RF; Southern VO.</li> <li>3) Military units of the JI, VAT, MP Black Sea Fleet, BF, PF, PKS, EW.</li> <li>4) “Division” of the Kuban Cossacks of the Russian Federation.</li> </ol>	<ol style="list-style-type: none"> <li>1) Seizure of local governments, law enforcement agencies.</li> <li>2) Capture of critical infrastructure objects (navigation control systems, main land highways).</li> <li>3) Blockade of military camps, air defence positions, bases of the Navy, airfields, establishment of control on the border with the Russian Federation.</li> <li>4) Introduction of regular troops to block PPD and fight against the Armed Forces, NGU.</li> </ol>

Organization and Management	Performers	The Main Measures of “Hybrid” Aggression
<b>4) Spontaneous actions of criminal elements</b>		
1) Criminal authorities of Ukraine and Russia.  2) Spontaneous actions of criminal elements for profit.	1) Crime of the RF and other republics of the former USSR.  2) Investigators of the RF sent by law enforcement agencies of the RF to Ukraine.  3) Pro-Russian criminal elements of Ukraine.  4) Offenders who were under investigation at the time of the aggression.	1) Pogroms of archives of law enforcement agencies (MIA, SBU, prosecutor’s offices).  2) Marauding, robbery of banks and private property.  3) Participation in hostilities as part of other gangs.  4) Seizure of weapons, ammunition and drugs.

**The first level:** The strategic idea of armed aggression was developed by the political leadership of the Russian Federation under the direct leadership of President Vladimir Putin in his role as the Supreme Commander-in-Chief of the Armed Forces of the Russian Federation. Direct planning, organization and comprehensive support was carried out by the Federal Security Service (FSB), the Ministry of Defence (MoD), the General Staff of the RF Armed Forces, the Armed Forces, Airborne Troops and the Southern Military District Headquarters.

**The second level:** The political platform for the hybrid aggression of the Russian Federation in Ukraine involved the Party of Regions, the Communist Parties of both Ukraine and the Autonomous Republic of Crimea, as well as pro-Russian parties and Crimean movements<sup>2</sup> within Ukraine. The main supporters and executors of the decisions of the separatist political forces were:

- Pro-Russian parts of the population in the eastern regions;
- Pensioners of “Soviet” orientation;
- Representatives of the criminal business who were threatened with criminal liability for illegally acquired business; and
- Management of local governments, law enforcement agencies and the Armed Forces of Ukraine (AFU), which sided with the aggressor, etc.

Separatist political parties and movements formed the occupying authorities, organized the administration of the occupied territories, severely persecuted and destroyed Ukrainian patriotic organizations and their leaders under the guise of restoring the occupation “order”, organized rallies, rallies, etc. to support Russian aggression and to counter and undermine the legitimate government in Kyiv.

**The third level:** Application of the RF Armed Forces and other military formations in hybrid aggression. The general leadership of the military component of the aggression against Ukraine and the management of the plan for the strategic isolation of the military conflict was carried out by the Ministry of Defence, the General Staff of the Armed Forces and the FSB of the Russian Federation. The direct management of military aggression against Ukraine was carried out by operational groups of the Ministry of Defence, the General Staff (GS) and the FSB of the Russian Federation of the joint command posts of the Southern Military District and the Black Sea Fleet in Sevastopol.

---

<sup>2</sup> According to L. Grach’s interview on March 21, 2017; source: <https://meduza.io/feature/2017/03/21/esli-by-nas-ne-podderzhal-patrushev-v-krymu-stoyal-by-amerikanskiy-flot>

The basis of the Russian military formations involved in the aggression against Ukraine were troops (forces) drawn from the land forces; airborne troops; Marines of the Black Sea, Baltic and Northern Fleets; Agency of the Main Intelligence Directorate (GRU) of the General Staff and the FSB in Ukraine; and special purpose troops of the RF Armed Forces; paramilitary units of the Kuban Cossacks and illegal military formations created in the occupied territories, staffed by the pro-Russian, anti-state population of Ukraine and the “patriots” of the “Russian world” of the Russian Federation.

Regular units of the RF Armed Forces were used to block the military camps of the Armed Forces of Ukraine and those of the Internal Troops of the Ministry of Internal Affairs. Regular units also block access to/from facilities of particular significance such as airfields, seaports, air defence positions, air and sea navigation control systems, etc. In the Donbass territories, regular Russian troops formed the basis of hostilities against the Armed Forces of Ukraine. At the first stage, the “Cossack” units took part in the seizure of local self-government bodies and performed police functions in the occupied territories. Later they were used for protection and the defence of headquarters, artillery units, means of reconnaissance and electronic warfare, land communications, etc.

**The fourth level:** Spontaneous actions of criminal elements in the occupied territory and in other regions of Ukraine. Spontaneous pogroms were carried out by criminal elements from Russia, Ukraine, and other republics of the former USSR; offenders who were under investigation by Ukrainian law enforcement agencies, etc. The main purpose of such groups was to seize archival and other documents from the files of the Ministry of Internal Affairs, the Security Service of Ukraine, and the courts. Some of them were destroyed on the spot or sold to interested criminals; the more important ones were selected by the FSB agency (mostly documents from the SBU archives). Spontaneous actions consisted of pogroms of banks, trade establishments for the purpose of profit. The main targets for the criminal elements were warehouses with weapons, ammunition and drugs.

One of the features of hybrid aggression against Ukraine is that the military formations of the Russian Federation were introduced only in regions where the local population’s support for the “Russian world” exceeded 50%.<sup>3</sup> Thus, in Dnipropetrovsk, Zaporizhia, Kherson, Kharkiv and other south-eastern regions of Ukraine, the aggressive plans of the Russian leadership failed due to low support for aggression by the local population and high activity of Ukrainian patriotic forces.

Summarizing the above, it should be noted that in the context of a possible large-scale invasion by the Armed Forces of the Russian Federation into the territory of Ukraine, it would be critical to organize the components of Ukraine’s defence system – especially that of Territorial Defence (TrD) – against hybrid threats.

### **3.3 TERRITORIAL DEFENCE OF UKRAINE**

The organization of the defence system of Ukraine since the beginning of the Russian military aggression in 2014 is insufficiently studied and needs in-depth analysis. This analysis builds upon the four main areas of threat to the national interests of Ukraine and the sequence of major measures of Russian hybrid aggression outlined above. Territorial defence as a component of Ukraine’s defence system also needs to be better understood in order to organize effective counter action to a possible invasion by the Russian Armed Forces. In part, an analysis of the existing system of countering threats to the national interests of Ukraine and ways to improve it were considered by the authors in Ref. [1].

---

<sup>3</sup> According to the official website of the CEC of Ukraine: <https://www.cvk.gov.ua>

At the same time, it is necessary to single out the measures that were spontaneously carried out by patriots in most regions of Ukraine since the beginning of the Russian aggression. The main ones were:

- 1) The personnel of the military reserve mobilized independently and en-mass so the commissariats could deploy them to the Armed Forces;
- 2) Representatives of the most active part of the reserve forces formed volunteer battalions, which independently moved to Donetsk and Luhansk oblasts to repel the invasion of Russian troops into the territory of Ukraine;
- 3) Once significant problems in securing troops in the shortest possible time were identified, a volunteer movement was formed, which played a significant role in maintaining the combat capability and welfare of military units of the Armed Forces during the hostilities of 2014 – 2016;
- 4) In the settlements of almost all regions of Ukraine, checkpoints were independently established which took control of the movement of people, the transport of goods, and strengthened the protection of critical infrastructure of the state.

Thus, with the beginning of the Russian hybrid aggression against Ukraine, a system of nationwide resistance spontaneously formed. At the same time, in regions where pro-Russian parties and movements had the support of the population, anti-Ukrainian paramilitary organizations and illegal armed formations were created under the leadership of the GRU General Staff and the FSB. During these spontaneous actions of self-defence by the population, some thoughts developed as to which elements of the organization of territorial defence needed to be considered by commanders of the AFU for development as the basis of new system to counteract modern methods of Russian hybrid war.

In recent years, the legislative work on the organization of territorial defence of Ukraine has intensified. Several bills were developed and submitted to the Verkhovna Rada of Ukraine. In pursuance of the Law of Ukraine “On National Security of Ukraine” and in accordance with the provisions of the Military Security Strategy approved by the Decree of the President of Ukraine No. 121 of March 25, 2021, the state introduced the principle of comprehensive defence. The key elements of which are steady resistance the full potential of the state and society. On this matter, the draft Law “On the Fundamentals of National Resistance” (No. 5557, registered on May 25, 2021),<sup>4</sup> submitted by the President of Ukraine and adopted as a basis with a reduced period of preparation [7], is particularly relevant. This draft law should regulate the development of territorial defence, the organization of the resistance movement and the appropriate preparation of the citizens of Ukraine for national resistance – this being an integral part of the comprehensive defence of the state throughout Ukraine.

One of the leaders in creating a system of territorial defence abroad today is Poland [8], [9], [10]. The Territorial Defence Forces (Polish: *Wojska Obrony Terytorialnej*) is one of the five types of Polish Armed Forces, the formation of which began in 2015 and now numbers 53,000 service personnel. Crucially, TrD do not belong to the military reserve, service in these troops is a type of actual military service. TrD forces cover 17 territorial defence brigades: one in each of the 16 voivodeships and two in the Masovian voivodeship.<sup>5</sup> On March 18, 2021, the Minister of Defence of Poland decided to create three additional Troop brigades; the total number of troops remains unchanged.<sup>6</sup> This method of organization bears a resemblance to that laid out in the draft Law on the Fundamentals of National Resistance submitted by the President of Ukraine to the Verkhovna Rada of Ukraine on May 25, 2021. Poland, as a NATO member state, is in NATO’s overall defence system, while Ukraine must rely on its own forces. Accordingly, the tasks and structure of our defence systems, in particular territorial ones, differ.

---

<sup>4</sup> On August 1, 2021, the Law of Ukraine No. 1702-IX “On the Fundamentals of National Resistance” came into force, which came into force on January 1, 2022. The document was officially published in the newspaper *Golos Ukrainy* on July 31, 2021 – Ed.

<sup>5</sup> *Wojska Obrony Terytorialnej*. – <https://terytorialsi.wp.mil.pl>

<sup>6</sup> *Serwis Rzeczypospolitej Polskiej*. – <https://www.gov.pl>

The analysis of the creation of TrD systems in Ukraine revealed that its main problems are:

- 1) Restrictions on the state budget for financing the security and defence sector. Conducting hostilities in the east of the country requires Ukraine to focus significant financial costs on the maintenance, development and reform of the ZSU.
- 2) In Ukraine, a significant number of the population, especially in the south-east, supports the pro-Russian vector of state development. Control over private, pro-Russian media in Ukraine enables the Russian Federation to carry out large-scale information operations which negatively affects the patriotism of the population and the personnel of the Armed Forces. In the process of forming TrD units, it is necessary to conduct a careful subdivision of personnel, taking into account the party affiliation and political views of the candidates.
- 3) The presence of anti-Ukrainian political parties and movements that support the hybrid aggression of the Russian Federation. The number of pro-Russian political parties and movements in Ukraine is growing, their influence on the population is spreading, especially in the south-eastern regions. This conclusion is confirmed by a comparative analysis of the results of local elections in 2015 and 2020 in the four southern regions of Ukraine<sup>7</sup> (Table 3-2).
- 4) In our opinion, the proposed draft Law “On the Fundamentals of National Resistance” violates one of the basic military principles. Namely that the structure of territorial defence, especially the brigade-level formation, must have a reliable, rigid system of management and comprehensive support. Of particular concern within the law are the provisions of Article 1 “Definition of basic terms”, Article 7 “Management of national resistance”, and Article 16 “Powers of headquarters of zones (districts) of territorial defence, heads of zones (districts) of territorial defence”. These provide (civilian) heads of regional, local, and district state administrations the right to manage military units.
- 5) The objectives of Russian military exercises show that command staff prepare for a strategic coastal operation. The main objectives of the Southern Military District may be:
  - The separation of Ukraine from the Black Sea and the seizure of coastal infrastructure;
  - Complete mastery of the waters of the Sea of Azov; and
  - Restoration of water and energy supply to the Crimean peninsula from the territory of the Kherson region.

**Table 3-2: Comparative Analysis of the Results of Local Elections in 2015 and 2020 in the Four Southern Regions of Ukraine.**

No.	Regions of Ukraine	Elections 2015 (Opposition bloc) %	Elections 2020 (OPZZh, “Sharia Party”) %	Share Growth %
1	Odessa	27.38	35.71	+8.33
2	Mykolaiv	26.56	37.65	+11.09
3	Kherson	20.31	43.74	+23.43
4	Zaporozhye	33.30	47.69	+14.39

<sup>7</sup> According to the official website of the CEC of Ukraine – <https://www.cvk.gov.ua>



As can be seen from this assessment of the regional security environment, Russia has deployed forces from the Southern Military District against Ukraine with a clear strategic objective in mind. Ukraine, on the other hand, is able to create and maintain a system of defence tailored to counter the specific methods of “hybrid” aggression by the RF in the south-eastern region of the state. This includes the formation of a single strategic group of forces to repel any invasion by the Russian Southern Military District. In another territory of Ukraine, it is expedient to organize the system of territorial defence of the state in accordance with the specific conditions and likely RF methods in this territory. It is important to now organize systems of territorial defence in other regions of the Ukraine that are equally tailored to meet the expected/demonstrated threat from Russian forces. Historical experience shows that territorial defence is one of the most difficult aspects of warfare. Much depends on the strength of the enemy’s military potential and an in-depth analysis of their methods of military action but consideration must also be given to the domestic political situation. The main purpose of territorial defence is to strengthen the state’s defence capabilities by making use of the resources of local governments and those patriotic citizens who are not already subject to mobilization.

### **3.4 TERRITORIAL DEFENCE PRIORITIES**

Given the threat of Russian hybrid aggression, it is expedient to develop Ukraine’s defence in four main areas:

- 1) Intensification of defence reform measures in order to accelerate the accession to the NATO military-political bloc and the development of cooperation with the member states of the Euro-Atlantic Alliance.
- 2) Organization of active and large-scale counteraction to Russian information and cyber operations directed against Ukraine.
- 3) The creation of a modern Armed Forces based on NATO principles, as part of highly mobile, joint, operational and tactical units- on the basis of which it is advisable to form an interspecific strategic group of forces organized under a single command and control, with the latest system of comprehensive military operations. The strategic forces of the Armed Forces of Ukraine must be able to successfully resist the offensive operations of groups of troops (forces) of the Southern Military District of the Russian Federation.
- 4) Formation of a modern system of territorial defence, integrated into the general defence system of the state under the leadership of the General Staff of the Armed Forces. These should be able to successfully maintain martial law whilst also organizing the reliable protection and defence of critical state infrastructure (especially military).

According to Article 18 of the Law of Ukraine “On Defence of Ukraine” [11] “territorial defence of Ukraine is a system of national military and special measures carried out in a special period.” The areas of responsibility for the subjects of territorial defence are closely connected and depend on the military-administrative division of the state. As stated in the draft law “On the basis of national resistance”, the main tasks of territorial defence can be [7]:

- 1) Participation in strengthening the protection and defence of the state border;
- 2) Participation in the protection of the population, territories, the environment and property from emergencies including recovery in the wake of military (combat) operations;
- 3) Participation in the preparation of citizens of Ukraine for national resistance;
- 4) Participation in the provision of conditions for the safe functioning of state authorities, other state bodies, local self-government bodies and military administration bodies;
- 5) Participation in the protection and defence of lines of communications and other critical infrastructure, as determined by the Cabinet of Ministers of Ukraine;

- 6) Providing conditions for the strategic and operational deployment of forces or their regrouping;
- 7) Participation in the implementation of measures to temporarily prohibit or restrict the movement of vehicles and pedestrians near and within the zones / areas of emergencies and / or the conduct of military (combat) operations;
- 8) Participation in ensuring public safety measures and public order in settlements;
- 9) Participation in the introduction and implementation of measures relating to martial law in the event of its legal imposition on the entire territory of Ukraine or in some of its localities by the government;
- 10) Participation in the fight against sabotage and reconnaissance forces, armed formations of the aggressor (enemy) and any other illegal paramilitary or armed formations; and
- 11) Participation in information activities aimed at increasing the level of defence capabilities of the state and to counteract the information operations of the aggressor (enemy).

To perform the proposed tasks, it is advisable to have two components in the TrD troops: the first – combat personnel; the second is the supply system. The fighting force of the TrD troops should include units designed to combat enemy sabotage and reconnaissance groups, airborne troops, search and capture of terrorist groups, protection and defence of important objects. It is expedient to involve departmental security units in the combat staff. The supply system of TrD troops should include: car repair companies, regardless of ownership; road repair; bridge construction; SES units; and other structures, according to their purpose.

The number and structure of both combat units and support groups depend on the specific tasks of the TrD and the conditions of the military-political situation in the area of responsibility of their respective territorial command (TRC). According to the Decree of the President of Ukraine No. 39/2016 of February 5, 2016 [12]:

*military-administrative division of the territory of Ukraine is the delimitation of the territory of the state into military-administrative zones (districts) in the interests of Ukraine's defence. The military-administrative division of the territory of Ukraine determines the territorial division of responsibilities and powers of the military administration of the Armed Forces of Ukraine in the field of state defence on land, in air and sea.*

Thus, the military-administrative division of the state is carried out in the interests of the command and control system of military forces and depends entirely on specific threats to the territorial integrity of Ukraine. Based on the military-terrorist actions of the RF Armed Forces, including the FSB, the most expedient distribution of TrD zones may be according to the identified methods of enemy hostilities. The first zone – TrCom “East,” will be concerned with hostilities with the regular forces of the Russian Federation. The second – TrCom “Center”, will concern itself with counteraction to the reconnaissance and terrorist actions of the Russian Federation. The third – TrCom “West,” will have responsibility for combating the intelligence and information activities of the enemy. Thus, in accordance with the real military-political situation in Ukraine, in our opinion, the military-territorial division of the state should be clarified and determine the following division of TrD zones:

- TrCom “East”: Autonomous Republic of Crimea, Kharkiv, Luhansk, Donetsk, Dnipropetrovsk, Zaporizhia, Kherson, Mykolaiv, Odesa regions.
- TrCom “Center”: Chernihiv, Kyiv (excluding Kyiv), Zhytomyr, Poltava, Cherkasy, Kirovohrad, Vinnytsia, Khmelnytsky regions.
- TrCom “West”: Volyn, Rivne, Ternopil, Ivano-Frankivsk, Chernivtsi, Zakarpattia, Lviv regions.
- A separate zone of TPO “Kyiv” should cover sectors that are formed in the administrative districts of Kyiv.

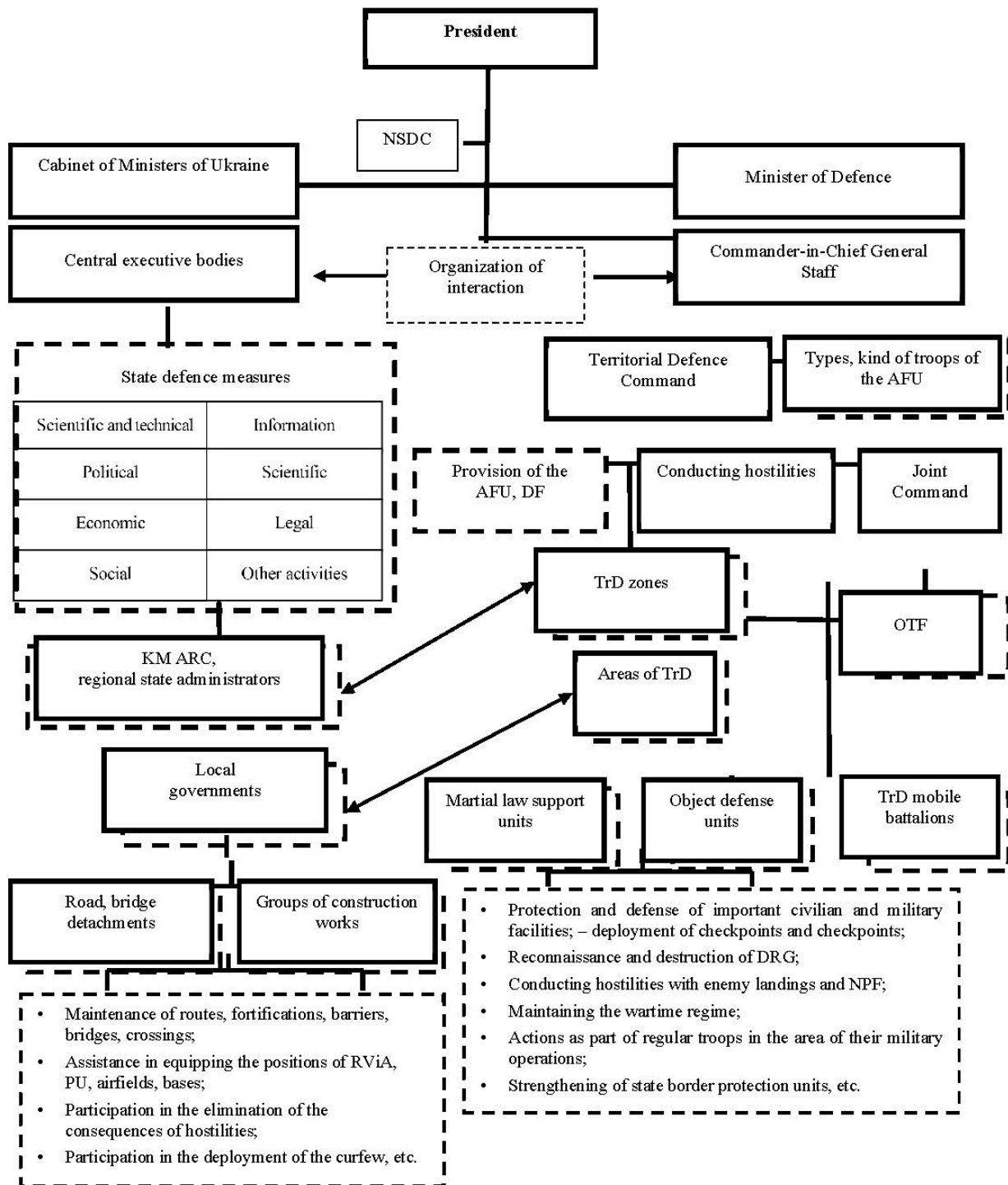
Each TrCom zone can be divided into sectors created within the administrative districts of the regions. The management and administration of the zones (sectors) will be carried out by the headquarters formed on the basis of the military commissariats (territorial centers of manning and social support). The organizational and staffing structure and the number of TrD units will depend on the specific conditions of:

- The military-political situation in the area of responsibility of the zone (sector);
- Anticipated options for enemy action in the area (sector);
- The presence, number and condition of security and defence forces (primarily the National Guard of Ukraine and the national police) in the assigned area of responsibility;
- The number of state and military facilities designated for protection and defence including the number of barrier areas and their characteristics, etc.; and
- The availability of free mobilization resources that can be involved in the recruitment of TrD, etc.

Thus, the formation of the structure and composition of TrD forces cannot be approached formally and bureaucratically and must remain flexible to account for the variables associated with each specific zone and sector. The role and place of each TrCom, zone and sector depend on many factors and cannot be the same in composition and number across Ukraine. The planning of the TrD is carried out by the General Staff of the Armed Forces of Ukraine on the basis of the decision of the Commander-in-Chief and approved by the Supreme Commander-in-Chief. TRCs are subordinated to the Commander of the Land Forces of the Armed Forces, who exercises direct command and management of territorial defence. TrCom “East” should be included in the Joint Forces and subordinated to the Commander of the Joint Forces. The data that informs the organization of the TrDs is one of the most important elements in planning their design. Military units associated with TrD cannot be larger than a battalion. To manage larger formations, such as a brigade, it is necessary to have well-trained and coordinated staffs, a reliable system of comprehensive support and many other features, of the absence of which can lead to desertion, looting of the local population and other chaos once hostilities commence.

In addition, TrD formations, as a rule, are part of the general system of comprehensive support of the Armed Forces and have costs comparable to similar regular force formations. This runs counter to ideas of carefully saving resources needed to ensure national defence. At the same time, the combat capability of TrD formations is significantly inferior to the combat capability of similar RF Armed Forces formations. One of the variants of the TrD structure is shown in Figure 3-2. The Ministry of Defence forms the initial data for the development of the TrD plan, namely: the list of critical infrastructure objects that are subject to defence strengthening (which is approved by the Cabinet of Ministers); conclusions on the assessment of state policy in the field of defence, the mobilization capabilities of the state to deploy TrD forces; a list of defence industry objects to strengthen their defence; submission of a state defence order for approval by the Cabinet of Ministers, submission of proposals to amend the Law of Ukraine “On the Budget of Ukraine” to ensure the defence of the state, etc.

The General Staff of the Armed Forces of Ukraine collects and analyzes the information necessary for planning and submits proposals to the Commander-in-Chief for a decision on the organization of the forces. Commands of the Armed Forces and the TRCom are involved in the planning of the TrD in the areas that concern them. TrD planning on the territory of the OS operation is carried out by the JF command as a section of the unified Plan of the TrD military operation and is approved by the Supreme Commander-in-Chief – the President of Ukraine. The individual commands of the zones and sectors carry out the planning of the TrD in their assigned territories: coordinating the allocation of forces and means for the TrD, the issue of logistical support and the deployment of the units of the TrD with local government bodies. Persons designated by the Commander of the Ground Forces of the Armed Forces are allowed to get acquainted with the full content of the TrD plans. In the area of the military operation this is at the discretion of the Commander-in-Chief of the Armed Forces.



**Figure 3-2: The Structure of the State TrD (Option).**

### 3.5 CONCLUSIONS

- 1) Ukraine is able to create and maintain a defence capability capable of resisting the “hybrid” aggression of the Russian Federation in the south-eastern region of the state, to form and provide one strategic group of forces to repel the invasion of the Southern Military District. In another territory of Ukraine, it is expedient to organize the system of territorial defence in accordance with the nature and methods of Russian military and terrorist actions in that territory.
- 2) The structure and areas of responsibility of the territorial defence system depend on the methods, ways and nature of expected military action from the enemy and form the basis of the military-administrative division of the state.
- 3) Organizational and staffing structures of territorial commands cannot be the same. They depend on variables such as the scope, number and importance of the tasks assigned to them, the expected combat operations of the enemy, the availability of mobilization resources, and the number of important objects intended for defence.
- 4) The expediency of forming TrD brigades is doubtful and requires separate scientific research and analysis. If the state is able to form about 24 TrD brigades and ensure their maintenance, it is more expedient to include them in the Armed Forces and additionally deploy operational and tactical groups of the Armed Forces in threatened operational areas.

### 3.6 REFERENCES

- [1] Frolov, V., and Semenenko, F. “Formation of a Promising Model of Organization of Defence of Ukraine.” *Science and Defence*, 3, 2019, pp. 3-9. <https://doi.org/10.33099/2618-1614-2019-8-3-3-9>
- [2] Illarionov A. “Challenges of Information Warfare for a Free Society and a Possible Counter-Strategy.” Speech at the XIX Estonian Open Society Forum. Tallinn, 18 September 2014. A. Illarionov, Livejournal. <https://aillarionov.livejournal.com/735489.html>
- [3] Snitsarenko, P., Zahorka, O., Pavlikovskyi, A., and Oksiiuk, O. “Cybersecurity as a Component of Information Security: Aterminological Aspect from the Point of View of the Ukrainian Information Legislation [Електронний ресурс]. *Problems of Infocommunications Science and Technology (PIC S&T): 2019 IEEE International Scientific-Practical Conference Proceedings*. K.: ФОП Андреев К.В., 2019, pp. 835-838. <https://doi.org/10.1109/PICST47496.2019.9061272>
- [4] “Security Passport of Ukraine – Results and Recommendations.” [Electronic resource]. DMGO Centre for International Security, National Institute for Strategic Studies, 2018. [https://intsecurity.org/Pasport\\_bezpeky\\_Ukrainy.pdf](https://intsecurity.org/Pasport_bezpeky_Ukrainy.pdf)
- [5] “Ukrainian Frontier: Challenges of Transcarpathia and the Black Sea Region.” [Electronic resource]: DMGO Centre for International Security, National Institute for Strategic Studies. [https://intsecurity.org/UAFrontier\\_UA\\_EN.pdf](https://intsecurity.org/UAFrontier_UA_EN.pdf)
- [6] “Ukrainian Frontier: Challenges for Tavria.” [Electronic resource]. DMGO Centre for International Security, National Institute for Strategic Studies. 2020. [https://intsecurity.org/ukrainian\\_frontier\\_vyklyky\\_dlya\\_tavriyi.pdf](https://intsecurity.org/ukrainian_frontier_vyklyky_dlya_tavriyi.pdf)
- [7] “On the Basics of National Resistance.” [Electronic resource]. Draft Law of Ukraine No. 5557, registration date 25.05.2021. Verkhovna Rada of Ukraine. Legislation of Ukraine, 2021. [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?Pf3511=72035](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?Pf3511=72035)

- [8] “National Security Strategy of the Republic of Poland [Електронний ресурс] 2020.” Biuro Bezpieczeństwa Narodowego. – Режим доступа, 2020. [https://www.bbn.gov.pl/ftp/dokumenty/National\\_Security\\_Strategy\\_of\\_the\\_Republic\\_of\\_Poland\\_2020.pdf](https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf)
- [9] Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022 [Електронний ресурс]: przyjęta uchwałą Rady Ministrów z dnia 9 kwietnia 2013. Biuro Bezpieczeństwa Narodowego. – Режим доступа, 2013. [https://www.bbn.gov.pl/ftp/dok/01/strategia\\_rozwoju\\_systemu\\_bezpieczenstwa\\_narodowego\\_rp\\_2022.pdf](https://www.bbn.gov.pl/ftp/dok/01/strategia_rozwoju_systemu_bezpieczenstwa_narodowego_rp_2022.pdf)
- [10] Koncepcja Obronna Rzeczypospolitej Polskiej [Електронний ресурс]: Maj 2017. Ministerstwo Obrony Narodowej. – Режим доступа, 2017. [https://archiwum2019-en.mon.gov.pl/p/pliki/dokumenty/rozne/2017/07/korp\\_web\\_13\\_06\\_2017.pdf](https://archiwum2019-en.mon.gov.pl/p/pliki/dokumenty/rozne/2017/07/korp_web_13_06_2017.pdf)
- [11] “On the Defence of Ukraine.” [Electronic resource]. Law of Ukraine No. 1932-XII of December 6, 1991, Verkhovna Rada of Ukraine. Legislation of Ukraine, 1991. <https://zakon.rada.gov.ua/laws/show/1932-12>
- [12] “On Approval of the Military-Administrative Division of the Territory of Ukraine. [Electronic resource]. Decree of the President of Ukraine No. 39/2016 of February 5, 2016, Verkhovna Rada of Ukraine. Legislation of Ukraine, 2016. <https://zakon.rada.gov.ua/laws/show/39/2016#Text>

## **Chapter 4 – MILITARY ASPECTS OF HYBRID WARFARE: THE UNITED KINGDOM AND OPERATION CABRIT**

**G.H.T. Reader**

Defence Science and Technology Laboratory (Dstl)  
UNITED KINGDOM

### **4.1 INTRODUCTION<sup>1</sup>**

This report has been produced in support of NATO SAS-161: *Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices*. It uses the experiences of the British Army deployments to Estonia on Operation CABRIT in support of the NATO Enhanced Forward Presence (eFP) as a basis for examining the military aspects of countering hybrid warfare. The report places these experiences within wider understandings of hybrid warfare in order to analyse them and contribute to understanding what role military capabilities have in countering hybrid warfare. The report was compiled prior to the Russian invasion of Ukraine in February 2022 but has been updated where required to address any resulting developments.

The report begins by explaining the historical context of recent British military deployments to Europe and how CABRIT relates to these. It then places CABRIT within the context of wider developments since the Russian annexation of the Crimean Peninsula in 2014 as this event provided the catalyst for the eFP. The hybrid activities experienced by UK forces deployed to CABRIT are then explored with a focus on understanding why these have been relatively limited. Examination of both UK military practices and UK-Estonian interactions are explored to outline ways in which NATO partners can make it difficult for military forces to be useful targets for hybrid activities. The report concludes with a discussion on the role of military forces in non-kinetic situations.

### **4.2 THE NATO ENHANCED FORWARD PRESENCE**

The groundwork for the NATO eFP was laid at the 2014 Wales summit of NATO members and was then further strengthened at the 2016 Warsaw summit [1], p.4. Since 2017 the UK has maintained a troop presence in Estonia as part of the wider NATO contribution to alliance security in Eastern Europe and the Baltic region. Of the four multinational battlegroups that constitute the eFP, the UK is the framework nation for the Estonian deployment, and it provides the largest contribution to the NATO force deployed there. [2] This troop presence is organised under the umbrella of Operation CABRIT and primarily deals with the deployment of an armoured battlegroup (approx. 800 – 900 personnel) to Estonia but also includes a smaller deployment to Poland (approx. 150 personnel). [3] This makes CABRIT the British Army's main effort in the Baltic region. However, CABRIT is not the sole UK effort aimed at ensuring alliance security in the region and should be considered alongside other UK military deployments<sup>2</sup> and relevant UK diplomatic or economic engagements. As an indication of how seriously the UK treats the eFP, the commitment of personnel to CABRIT was doubled in February 2022 when it became increasingly clear that large-scale Russian military action against Ukraine was imminent. This increased commitment was reaffirmed in June 2022.

---

<sup>1</sup> The author thanks those UK military personnel who agreed to be interviewed during the development of this chapter. Their experiences, insights, and comments were invaluable in drawing together events on the ground and wider theoretical understandings of hybrid activities. All such contributions have been anonymised. Similarly, some of the documents which this report draws upon cannot be released at the NATO UNCLASSIFIED, Public Release level of classification. Whilst the language of anything drawn from those documents has been suitably adjusted for this report, the documents themselves are not explicitly mentioned.

<sup>2</sup> Including: Op AZOTIZE (Baltic Air Policing Mission), Op Elgin (deployments to Kosovo), Op Tosca (deployments to Cyprus), and Exercise Cold Response (deployments to North Norway), Op INTERFELX (training of Ukrainian personnel), and the currently suspended Op ORBITAL (training deployments to Ukraine).

Since deploying forces to the eFP under CABRIT, the UK defence establishment has had to learn lessons about what have come to be known as hybrid activities<sup>3</sup> first-hand. Furthermore, the UK military has had to relearn certain skills that were deprioritised whilst the more counter-insurgency focused campaigns in Iraq and Afghanistan were being conducted.

### **4.3 PREVIOUS UK DEPLOYMENTS TO EUROPE AND CABRIT: HISTORICAL CONTEXT**

The central purpose of CABRIT and British contributions to the eFP remains unchanged from British NATO commitments during the Cold War. As with the British Army of the Rhine (BAOR) before it, CABRIT demonstrates the UK's commitment to NATO's principle of collective defence, provides reassurance to allies, and contributes to the deterrence of adversaries by denying them the freedom to act unopposed. In doing so, CABRIT demonstrates resolve to potential adversaries that an attack on one NATO member will be considered an attack against the alliance as a whole [4].

Under the *NATO-Russia Founding Act on Mutual Relations, Cooperation, and Security*, NATO declared that it would seek to ensure the integrity of the alliance through means other than the permanent stationing of substantial combat forces in theatre [5]. It is, therefore, unlikely that CABRIT will develop into something more akin to the BAOR without further significant developments that might call the Founding Act into question (such as the invasion of a NATO member state by a hostile power). However, sustaining CABRIT as an ongoing deployment just short of permanent stationing contributes to NATO solidarity by signalling the UK's lasting commitment to the alliance.

Like the BAOR before it, CABRIT is a deployment shaped by experiences, analysis, and lessons learned from a specific conflict. The BAOR's primary focus was on being prepared to conduct large-scale warfighting. That is to say, actions conducted by brigade, division, and corps sized mechanised combined-arms formations concerned with high-intensity warfighting across wide tracts of land in the shadow of nuclear escalation. In contrast, CABRIT is primarily concerned with an array of disruptive activities that might occur without recourse to the kind of fighting that was envisaged during the Cold War. This means that whilst the use of conventional forces is presumed likely in the case of a heightening of tensions, invasion by large-scale forces is presumed unlikely not least because of Estonia's status as NATO member. As a result, the forces deployed to CABRIT must be prepared to contend with both *potential* kinetic operations as well as *expected* non-kinetic activities. This being in addition to the latent effect the forces have, merely by deploying to another country as part of a NATO mission.

Since undertaking the CABRIT deployment, work has been conducted within the UK Ministry of Defence (MOD) that analysed the similarities and differences between the current situation and deployments undertaken during the Cold War by the BAOR. This work, and the lesson learning which has stemmed from CABRIT more widely, is rooted in an acknowledgement that the British military has been focused on counter-insurgency and stabilisation operations in contexts very different from that of the contemporary situation in Eastern Europe. As a result, the British Army has had to undergo significant revisions to best apply its capabilities to the challenges presented by a commitment to the NATO eFP.

### **4.4 FROM CRIMEA TO CABRIT: SHAPING THE MISSION**

CABRIT has a two-fold purpose: i) To reassure Estonia and other NATO allies; and ii) To deter Russian aggression. The first and more active of these purposes is primarily an information operation. Forces deployed to CABRIT must continually work to engage with target audiences, forge links with the Estonian

---

<sup>3</sup> This term is used to encompass those activities which make use of military elements, often in unconventional ways, in conjunction with sustained information activities and other elements of state power. Elsewhere, these may be referred to as hybrid warfare, sub-threshold activities, activities/operations in the grey zone, etc.



populace, and reinforce the reputation of the NATO mission. The second and more latent purpose of CABRIT is to deter adversaries from taking overtly hostile action against a NATO member nation by both providing a credible war fighting capability and by explicitly linking military action against Estonia to military action against the UK. The pursuit of these purposes requires an understanding of the complex threat facing the forces deployed to CABRIT. Firstly, there is the perceived threat to the battlegroup itself. This coming most prominently in the form of interference activities which harass, disrupt, or endanger personnel through non-kinetic means that primarily involve the use and misuse of information. Secondly, there is the perceived threat to NATO credibility and integrity that could come about from exploitable differences and misunderstandings between the host nation and the deployed force. Finally, there is the perceived threat to the host nation itself. Estonian concerns relate to the possibility of a short notice, rapid seizure of land akin to what happened to Ukraine with the Crimea.

Whilst not historically novel, the methods used during the Russian annexation of the Crimea and the Russian-backed conflict in the Donbas region brought hybrid activities to the forefront of NATO thinking [6]. Now, developing an understanding of how military activities best contribute to countering hostile activities below thresholds for armed conflict has become the subject of sustained study in the UK MOD. As a result, early deployments to CABRIT stressed the need to have as comprehensive an understanding of how likely adversaries operate as is possible. Observations like this led the UK MOD to conduct significant self-analysis of which applicable skills had atrophied since the Cold War and which have been strengthened. Whilst net-assessments of motivations, capabilities, and relative balances within a given context are a regular function of military activity, a developed understanding of adversaries is critical in situations characterised by constant competition below thresholds for armed conflict. Understanding perceptions of adversary behaviour is key to managing activities and counter-activities in a manner that avoids unintentionally escalating the situation above particular thresholds. This is an area in which it was recognised that the expertise and experiences of the host nation is an invaluable source for deployed forces to draw upon and learn from.

### 4.5 EXPERIENCES FROM CABRIT

The experiences of UK forces deploying to Estonia are rooted in the fundamentally different nature of CABRIT from those of Afghanistan or Iraq. Comparisons with Op TELIC and Op HERRICK are inevitable due to the central position they occupied in UK defence for an extended period of time. Those operations shaped how the British defence institution thought about adversaries, environments, and operations. This in turn defined how the British Army fought for a generation. Crucially, these operations also moulded the experiences and expectations of what military duty involved for many service personnel: frequent contact with adversaries and no shortage of kinetic operations. Some of those personnel not only still serve today but, in many cases, now occupy positions of greater seniority and influence than they did during those operations. This meant that during the initial CABRIT deployments, a certain amount of organisational inertia as to what Army life entailed had to be overcome. This has been achieved through a combination of targeted education and a sense of heightened threat awareness. Educating personnel about the situation in Eastern Europe has helped to provide understanding why CABRIT is an important operation despite its relatively calm character. Deploying to Estonia and spending time in-country has helped to raise awareness of non-kinetic threats and the dangers which stem from information activities. Developing an understanding of the context in which CABRIT takes place has been central to informing how forces deploying for the operation have adapted or developed skills and procedures to suit the demands of the mission.

Independent assessments of the Baltic region suggest that it would be difficult for an adversary to subvert the region without the use of conventional force [7]. This means that the worst-case scenarios for the region are those in which an adversary makes use, directly or indirectly, of conventional military forces. However, the initial CABRIT deployment identified risks in the digital environment and information activities as the most likely day-to-day threats. The information domain especially was considered a means that adversaries might

seek to exploit in order to damage the reputation of NATO through the eFP mission at low-cost and with little risk of inadvertent escalation. Early experiences of what may or may not have been nuisance activities conducted against the forces deployed to CABRIT were assessed to be largely insignificant in impact and notably less harassing than that experienced by other NATO eFP deployments. Similarly, low-level attempts at interfering with deployed personnel have been noted as being more mischievous than malign as they have not been sustained nor had a significant impact on the effectiveness of those forces, on UK-Estonian relations, or on NATO cohesion. Although difficult to assess, the low impact of these activities has been attributed to a combination of:

- A rigorous approach to the use of personal electronic devices (reducing exposure to risk);
- The success of outreach and integration activities (reducing opportunities for exploitation); and
- High quality of Estonian intelligence and cyber capabilities (increasing the difficulty for adversaries to operate).

In addition, the 2022 Russian invasion of Ukraine may suggest a fourth contributing factor. Namely, a lack of Russian understanding of targets/environments outside of those that were already favourable to their planned activities (Crimea/Donbas). It is acknowledged that the absence of serious incidents targeted at CABRIT may only indicate an unawareness of more significant intelligence activities taking place. Similarly, it is noted that the effort that an adversary commits to activities such as information operations is influenced by immediate political imperatives. As a result, it is unlikely that CABRIT will experience a noticeable increase in nuisance activities whilst Russia is pre-occupied with the war in Ukraine. Even if more significant activity has occurred without being detected, it has not yet been exploited in a manner which interferes with the operation of the forces deployed to the eFP or proved harmful to NATO more widely. Conversely, the absence of serious incidents could also be symptomatic of the successful deterrence of adversaries. The effects/outcomes of successful deterrence are notoriously hard to prove, however, so any such claims should be considered a possibility rather than a statement of fact.

The risk of continuous, highly effective, and highly damaging cyber-attacks against CABRIT is considered low. As a highly digitised country, Estonia is aware of the risks from malicious cyber-attacks, and has numerous ongoing initiatives that look to address malicious behaviour in this area. Estonia is also home to the Cooperative Cyber Defence Centre of Excellence – a NATO facility that contributes to the alliance’s cyber capabilities. This focus on defending against cyber activities stems from Estonia’s modern experience of having been targeted by a significant cyber-attack in 2007 [8]. Likewise, NATO more broadly witnessed what happened in Ukraine in 2014 and has since given more thought to cyber-attacks as a means for adversaries to achieve goals or support other operations. The lack of significant hostile activity directed at CABRIT in the information domain so far has not diminished perceptions of the seriousness that such threats pose to the eFP. Training continues to be conducted to raise awareness amongst personnel about the complexity of the threat. Exercises are conducted in-theatre that test the ability of the battlegroup to contend with an escalating variety of attacks in the information domain either directly against them or against the host nation which they could be drawn into.

#### **4.6 THE IMPORTANCE OF CULTURAL LINKS BETWEEN HOST NATIONS AND DEPLOYABLE FORCES**

Much was made at the onset of the eFP about the potential for forward-deployed forces to be exploited by the hybrid activities of adversaries as a means of creating tension between host nations and NATO allies [1], p.4. These perceptions were likely shaped by a combination of the freshness of Ukrainian experiences following the seizure of the Crimea in 2014, an assessment of possible worst-case scenarios, and the apparent novelty of hybrid approaches. The main areas of concern for such exploitation revolve around how deployed NATO troops might interact with civilian populations in the host countries including any ethnic Russian or Russian-speaking elements. This might take the form of misunderstandings stemming from

cultural frictions, being drawn into domestic unrest, or being the target of deliberately organised/supported violence [1], p.5. These represent a sliding scale of severity with the more severe outcomes only being possible if adversaries are able to exploit the earlier stages, i.e., organised violence against deployed forces is unlikely to achieve the desired effect if those forces are well integrated with the host population and there is little cultural friction. The British forces deployed to CABRIT have not had to concern themselves with domestic disturbances or organised violence within Estonia for several reasons. Firstly, Estonia has not experienced much in the way of serious domestic disturbance or targeted violence against foreigners and remains unlikely to do so in the near future based on current socio-political trends. Secondly, whilst the eFP is integrated into Estonian defence planning, they are not integral to all possible contingencies and so are less likely to be inadvertently drawn into such situations even if they were to occur. Finally, the ethnic Russian/Russian-speaking elements of the Estonian population have not served as the conduit for nuisance activities in the way that might have been feared following the 2014 annexation of the Crimea.

Deployments undertaken in support of other NATO missions, notably in Afghanistan, have seen British forces have to contend with an environment that was radically different from that with which they were familiar in the UK. In Afghanistan the land, the people, and the way of life were all alien to deployed personnel – factors that exacerbated, and were in turn exacerbated by, the nature of the mission. This was then further complicated by an adversary who made extensive use of the local populace for their own purposes. The same was true in reverse – British forces were alien to the local populations and so forces deployed to Afghanistan operated as highly visible strangers in a strange land. In Estonia, however, this is not the case. The major Estonian population centres, Tallinn in particular, are not markedly different to the casual observer from cities in the UK. English is widely spoken amongst the populace as a second language, especially amongst younger people who are widely taught it in school [9]. This has been especially useful for British forces deployed to the eFP given the difficulty in learning the Estonian language. Beyond the obvious usefulness of this widespread language training, knowing that younger people are more likely to speak English can serve as a useful indicator for deployed personnel as to who to speak with when facilitating social encounters with members of the local population.

This sense of familiarity also aids with facilitating engagement opportunities. When coronavirus restrictions limited both the more traditional in-country outreach activities and the ease for deployed units to rotate personnel back to the UK for rest and relaxation, this familiarity proved valuable. Units were able to organise in-country relaxation periods that were well received by both the military personnel taking a break from active duty and by the local population who benefitted from the influx of custom into otherwise closed sectors of the economy (hospitality). This sort of opportunity would not have been possible without i) A developed understanding of the threat picture based on experience; and ii) The receptiveness of the host population to foreign service personnel.

Detailed knowledge of the Baltic region amongst British forces personnel is not extensive and so initial understandings of what to expect when deploying are limited. However, Estonia is a popular holiday destination for British tourists and so elements of the Estonian population have a passing familiarity with British mannerisms and are used to the presence of British people [10]. Once it becomes clear to the personnel involved with CABRIT that Estonia is not as different from the UK as pre-deployment misconceptions might suggest, the nature of the reassurance mission becomes easier. The effect of this is two-fold: Firstly, UK personnel do not, through their presence or their conduct, stand out from their human surroundings in Estonia in the same way as forces deployed to Afghanistan or Iraq did. This means that cultural misunderstandings are infrequent and those that do occur are limited in severity. Therefore, interactions between British personnel and the Estonian people do not provide much opportunity for significant exploitation by adversaries. Secondly, deployed forces are not pushed into a siege mentality wherein everything beyond their fortified camps seems different, unwelcoming, and hostile – a course of action that would isolate them from the local populations they are meant to be reassuring. This relative ease of understanding between the host population and the deployed forces provides an inherent resilience for the NATO mission against activities that seek to cause friction between the two. As an ongoing commitment,

CABRIT has now reached an important phase in regards to familiarity with the host nation that will continue to maintain these links. Units are starting to deploy to the eFP for the second time. This means that there will be greater organisational awareness within the battlegroup and the transition to in-theatre activities will be more efficient with an accompanying reduction in the likelihood of points of friction. The basic elements of life for both British personnel and the local population have started becoming more normalised, freeing CABRIT personnel to focus on the key aspects of the mission.

Estonian efforts to enable smooth cooperation with NATO partners have undoubtedly played a significant role in this. The Estonian national context makes such integration a serious matter that drives planning and development considerations in defence and security. Furthermore, Estonian military personnel previously deployed to Afghanistan alongside UK forces during Op HERRICK. This means that there were a number of organisational links between the two prior to the first CABRIT deployment which eased the period of initial integration. Similarly, Danish forces had also worked with the UK in Afghanistan so the multinational battlegroup that comprises the eFP in Estonia has a sense of shared operational experience beyond their immediate role and has been able to utilise a sense of shared corporate memory.

#### **4.7 UNDERSTANDING INFORMATION ACTIVITIES**

Countering and pursuing objectives that may focus on areas beyond the traditional purview of military forces whilst in competition with adversaries requires a combined approach and the military has an important part to play in this. The success of subversive militarised activities outside of armed conflict hinges upon the capabilities of the perpetrator and the impotence of the victim. This impotence results from a combination of: i) The inability to prevent the action itself; and ii) An inability to impose sufficient cost upon the perpetrator to affect their decision making such that they do not take the action in the first place. The eFP assists with both of these by potentially plugging capability gaps and demonstrating NATO's commitment to Article 5. It is not expected that the forces deployed to CABRIT should be able to halt an all-out attack upon Estonia by a peer-plus adversary since this is not the primary purpose of the eFP. Instead, the purpose of UK forces deployed as part of CABRIT is to deter such an attack from occurring in the first place. They achieve this by: i) imposing upon adversary decision making the very real cost and implications of attacking a NATO member and ii) assisting in countering hostile activities which occur below thresholds for armed conflict, but which may seek to achieve goals traditionally pursued through open warfare. Since the latter relies, in part, upon the credibility of the former, and both rely upon the capabilities of conventional forces, it is crucial for the forces involved with CABRIT to ensure that their tactical activities contribute to strategic effects where possible. However, CABRIT is simply one aspect – the British Army aspect – of more nuanced, whole of government/cross-alliance approaches to countering hybrid activities. Within that wider framework, the forces deployed to CABRIT do engage with hybrid activities but do so in a manner consummate to their capabilities and with realistic expectations of what they might achieve. A recent CABRIT deployment listed six areas of focus for the battlegroup. Of these, all six were pertinent to war fighting whilst only three could be said to have value without consideration for armed conflict. This is not to say that the forces involved in CABRIT are not conducting activities pertinent to the perceived threat but, rather, this underlines the importance of understanding what the real threat is, acting accordingly, and not losing sight of achievable objectives.

Based on the deployment of forces to CABRIT and wider understandings of constant competition between states, work has been conducted on how the armed forces can make best use of the information environment to counter hostile activity. This work has shown that information and outreach activities conducted primarily through social media may be limited by experience and understanding of the wide array of platforms in use and how to make best use of them. Such activities require sufficient understanding of target audiences as well as working knowledge of the forms of engagement that different forms of social media best enable relative to those audiences – especially the Estonian population. Furthermore, adversaries may conduct activities on platforms that service personnel have limited access to, or they might make use of platforms that

are wholly unsuitable for official accounts to be communicating through. It has been suggested that with sufficient training and understanding in these areas, or through the more widespread inclusion of specialists, units would more likely be pre-authorised to conduct this sort of engagement without recourse to lengthy chains of communication to get authorisation.

These developments have built upon early assessments that UK military understanding and implementation of influence activities had previously been slow and incoherent. Since this was constraining the ability of units to understand target audiences, counter false anti-NATO narratives and analyse trends in adversarial information/disinformation activities (a vital preparatory activity), this was identified as an area for development [11], p.46. It was assessed that command and control activities in the information environment were best suited to analytical tasks (of target audiences) with some potential for monitoring and evaluating adversary activities. Understanding the true level of genuine engagement (rather than artificial amplification) of the latter can be time consuming, which makes formulating direct responses complicated [11], p.54. As a result, it is better to ensure that the relationship between the eFP and the host nation is robust enough that it is difficult for easily amplified misinformation to gain traction. Likewise, it has been identified that media training within the eFP – both how to create effective media and how to interact with other media agencies – is required prior to deployment and that this is an area where there is room for continual improvement. Further work has shown that within units tasked with operating in the information environment<sup>4</sup>, dogmatic thinking is overly restrictive and hierarchical planning processes are too time consuming to produce effective results. Given that timely activity is critical in the information sphere, working environments in which it is safe to fail and in which challenges to accepted thinking are encouraged are seen as important for developing free-thinking approaches to the risks of the information environment.

The ability of the eFP to conduct information and outreach activities has been augmented by the inclusion of specialist teams attached to the deployed forces. From the beginning of the CABRIT deployment, community outreach activities have been a key undertaking alongside honing the warfighting capabilities of the battlegroup. At every opportunity the deployed forces have sought to amplify these activities through both traditional and digital media. The specialist teams provide embedded expertise on how the CABRIT battlegroup can most effectively leverage their presence and engagements with the Estonian people into effective media coverage. These are used to reinforce positive perceptions of NATO and counter the malign information activities of adversaries. Ordinarily these activities would be divided between physical engagements, use of official social media channels, and appearances in more traditional Estonian media. Physical engagements, such as appearances at local events and military-themed fitness sessions, being the favoured approach since they allow for the most impactful connection between UK troops and the Estonian population. The CABRIT battlegroups adapted to the onset of COVID-19 by increasing their digital engagement activities to compensate for the restrictions on physical events. The ability to continue to conduct limited physical events (within social distancing guidelines) throughout this period is testament to both the strong links which CABRIT has maintained with key figures within Estonian society and the high regard with which NATO engagement events are held by Estonians.

Politically, the deployment of the British-led NATO eFP to Estonia was described by the Estonian Defence Minister as one of the most important events in the country's recent history. The initial deployment of forces to CABRIT also attracted a significant number of high profile visits from both Estonian and international officials. An important point that has been observed by forces deployed to CABRIT is that the information activities conducted by the forces deployed there should not become overly fixated on broad audiences. Particular forms of engagement with smaller audiences such as these high profile visits may have impact that extends beyond the immediacy of that audience – e.g., wider engagement with the host nation military beyond the units integrating with the eFP. The February 2022 announcement in which the UK declared that it would double the personnel committed to CABRIT contributed to this political messaging by signalling to

---

<sup>4</sup> This is taken to encompass both those units whose primary functional activities concern the information domain (e.g., PSYOPS) and those units who are temporarily tasked with conducting such activities (e.g., media engagement, public relations, etc.) whilst remaining ready to fulfil their primary function.

adversaries that NATO would not idly observe the escalation of military activities in Europe. The June 2022 reaffirmation of this increased commitment was publicly announced in a joint statement by the Prime Ministers of both the UK and Estonia. Something which, again, signalled the unity of purpose between the host nation and international NATO partners. Such signalling is directed equally at domestic audiences, international allies across NATO, and at adversaries who might question NATO solidarity.

#### **4.8 MILITARY PERSPECTIVES FOR THE FUTURE**

In the time since Op CABRIT began, the British Army has fundamentally rethought its approach to operations. The MOD's recent *Integrated Operating Concept 2025* (IOpC) outlines four broad phases of activity in which it expects to operate [12], p.11. Three of these four can occur below thresholds for armed conflict and thus outside of the traditional purview of the military instruments of state. Although the IOpC deals with familiar concepts (operations other than war, counter-insurgency operations, etc.), it serves to raise the importance of combating adversaries without the Army itself actually fighting. If, however, the IOpC serves its purpose and helps to shape how the Army conceptualises its role in persistent competition, then it marks an important step in understanding the part the military has to play in whole of government approaches to complex problems.

Much analysis has been produced on the conduct of adversaries and how to protect against hybrid activities. Views from within the British Army are that whilst this work is good it has so far been grounded in a very reactive approach [13], p. 27. Responding to the actions or methods of others is seen as one element of what should be a more encompassing approach and so the British Army has begun to explore more proactive ways in which military forces can contribute to generating persistent competitive advantage. This is dependent upon maintaining an accurate understanding of the motivations, capabilities, and intent of adversaries alongside awareness of the perspectives of allies, and rigorous self-assessment. Key amongst this is the notion of flexible force structures which provide mass for the 'once in a generation warfight [sic]' but which can provide key capabilities at the critical level for other operations [13], p. 31. Notably, these approaches still build upon the same foundation as more reactive approaches. Namely that for military forces to contribute effectively to hybrid activities they must be representative of credible warfighting capabilities [13], p. 29. For forces deployed to the eFP to contribute to deterrence, the plan to support those forces should the need arise must also be credible. If an adversary assesses that the deployed force is isolated or that it lacks support which could provide extra capabilities or additional mass in a timely fashion, then the deterrence function of that force becomes questionable. Since the purpose of the eFP is to enhance deterrence, efforts have been made that ensure the support plan for CABRIT is robust. In 2019, Op TRACTABLE was conducted to rigorously test the movement of material from the UK to Estonia in a timely fashion. As well as the material function in such an exercise, this reinforced the seriousness with which the UK views its commitment to the eFP by demonstrating the depth of capabilities which support CABRIT.

Having forward-deployed forces in an important theatre provides opportunities for experimentation with new or developing capabilities and practices in a more appropriate environment than might be found in other training areas. This has enabled the validation of findings from virtual or simulated training conducted elsewhere in the MOD. Furthermore, the interactions of deployed forces with host nation forces in a semi-live environment allows for detailed exploration of the force design for an eFP. This means the aims, composition, and doctrine of the eFP are able to adjust in response to developments as and when necessary. Similarly, the ground over which the eFP might expect to have to fight in the event of a conventional attack features many key areas that are largely unchanged since they were fought over in the 20<sup>th</sup> century. This, coupled with the fact that likely adversaries are familiar with the terrain, means that historical analysis of the region has a more direct application to military operations than is sometimes the case.

## **4.9 CONCLUSIONS, KEY TAKEAWAYS, AND LESSONS FOR OTHERS**

Whilst military forces may be used as part of wider efforts to conduct/counter hybrid activities, warfighting remains the primary purpose of such forces. It is their ability to fight wars that makes them a distinct capability for governments seeking to employ all elements of state power in the conduct of hybrid activities. Therefore, the overriding aim of using military forces in situations which are below thresholds for armed conflict should be to provide credible deterrence. This is achieved by: i) policy makers making sure that clear, identifiable, and credible thresholds exist and ii) ensuring that adversaries cannot achieve particular objectives without crossing those thresholds. By maintaining credible conventional forces within member nations, NATO ensures that it diminishes avenues by which an adversary might most effectively make use of its own military to achieve goals. Diminishing the risk of open conflict makes the pursuit of non-military initiatives that contribute to wider regional stability and prosperity more feasible [7], p.31. CABRIT reinforces the renewed importance of credible conventional military capabilities. These capabilities provide the bedrock for less conventional uses of the military below thresholds for armed conflict, so the honing of these skills is of fundamental importance to countering hybrid activities. Any efforts to expand what military forces can do beyond their core areas of responsibility (such as conducting sub-threshold activities) must be balanced against any potentially detrimental impact on core capabilities (warfighting). CABRIT deployments continue to stress the need to develop information activities so that forces can continue to engage key audiences using a variety of forms of media. The development and inclusion of specialists trained in these areas will enable empowered units to conduct more of these activities without having to request authorisation.

Based largely on the experiences of Ukrainian forces engaged on the Donbas front during the 2014 – 2022 conflict, expectations prior to the commencement of CABRIT were that forces deployed there would have to contend with significant attempts by adversaries to undermine Estonia-UK relations via interference activities. This has not been the experience of British forces deployed to the region. The most significant experiences the UK has had of hybrid activities since CABRIT began have occurred within the UK itself and not through the deployed forces. These experiences have ranged considerably in character. There have been widespread misinformation campaigns surrounding key societal events, such as the 2016 referendum on leaving the European Union, which have sought to influence British public opinion. There have also been chemical weapons used on UK soil as in the attempted assassination of Sergei and Julia Skripal in 2018 using the Novichok nerve agent. These experiences reinforce the idea that hybrid activities, whilst containing military elements, are not restricted to the interplay of armed forces across conventionally understood battlespaces.

That the forces deployed to CABRIT have experienced little meaningful hostile activity suggests that the experiences of hybrid activities by NATO members will vary on a case-by-case basis. Furthermore, such experiences will be influenced heavily by the intent of adversaries at any given point in time and the situational context. For this reason, it may be that experiences will be fundamentally different for nations deploying into the region than that of the host nations. Since CABRIT is seen as one part of wider UK and NATO efforts, its conduct is managed accordingly. This requires a meaningful level of integration and familiarity between UK and Estonian personnel to successfully achieve. Thankfully historical, cultural, and social connections between Estonia and the UK do not provide obvious points of weakness for adversaries to exploit through subversive activities. The possibility that more significant activity has occurred without being detected cannot be ruled out. However, since such activity has not been exploited in a manner which interferes with CABRIT or harms NATO more widely, its usefulness in the future would be limited. With acknowledgement that successful deterrence is notoriously hard to prove, the absence of serious incidents may also suggest that CABRIT has successfully reinforced NATO deterrence in the region.

#### **4.10 REFERENCES**

- [1] Zapfe, M. “ ‘Hybrid’ Threats and NATO’s Forward Presence.” Policy Perspectives 4(7), 2016.
- [2] NATO. “NATO’s Enhanced Forward Presence.” Fact Sheet, 2020 [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2020/10/pdf/2010-factsheet\\_efp\\_en.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2020/10/pdf/2010-factsheet_efp_en.pdf) Accessed: February 2021.
- [3] British Army. “Deployments: Baltics.” 2020. <https://www.army.mod.uk/deployments/baltics/> Accessed: February 2021.
- [4] Supreme Headquarters Allied Powers Europe. “Enhanced Forward Presence.” (2020). <https://shape.nato.int/efp> Accessed: February 2020.
- [5] North Atlantic Treaty Organization. “Founding Act on Mutual Relations, Cooperation and Security between NATO and the Russian Federation signed in Paris, France.” 1997. [https://www.nato.int/cps/en/natohq/official\\_texts\\_25468.htm](https://www.nato.int/cps/en/natohq/official_texts_25468.htm) Accessed: April 2021.
- [6] Molloy, M. “Increasing the Cost for Russian Hybrid Activity: Opportunities for NATO Success.” The College Series, 12 NATO Defense College, Senior Course 136, February-July 2020. <https://www.ndc.nato.int/download/downloads.php?icode=687> Accessed: March 2021.
- [7] Radin, A. “Hybrid Warfare in the Baltics: Threats and Potential Responses.” RAND Corporation, 2017. [https://www.rand.org/pubs/research\\_reports/RR1577.html](https://www.rand.org/pubs/research_reports/RR1577.html) Accessed: February 2021.
- [8] Tamkin, E. “10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?” Foreign Policy, 27 April 2017. <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/> Accessed: April 2021.
- [9] Republic of Estonia Ministry of Education and Research. “Foreign Language Learning in Estonia.” 2020. Available at: <https://www.hm.ee/en/activities/estonian-and-foreign-languages/foreign-language-learning-estonia> Accessed: April, 2021.
- [10] Breaking Travel News. “Estonia Sees British Visitor Figures Increase by a Fifth.” 27 February 2018. <https://www.breakingtravelnews.com/news/article/estonia-sees-british-visitor-figures-increase-by-a-fifth/> Accessed: April 2021.
- [11] Reindorp, D. “Command and Control of the Information Environment.” Niteworks. NW/PR/0950/008, 2017.
- [12] Ministry of Defence “Introducing the Integrated Operating Concept.” Ministry of Defence, 2020. <https://www.gov.uk/government/publications/the-integrated-operating-concept-2025> Accessed: April 2021.
- [13] Tedman, P., and English, N. “The Utility of Combat Aviation in the 21<sup>st</sup> Century: Exploiting Aviation Manoeuvre.” British Army Review, 178, 2020.



## Chapter 5 – CASE STUDY OF RUSSIAN HYBRID ACTIVITIES IN THE CZECH REPUBLIC

**Jan Bren**

University of Defence, Centre for Security and Military Strategic Studies  
CZECH REPUBLIC

with significant contributions from

**Petr Matous**

Czech Ministry of Defence  
CZECH REPUBLIC

### 5.1 STRATEGIC APPROACH OF THE RUSSIAN FEDERATION WHEN USING “HYBRID INFLUENCE”

This chapter is aimed at the issues of strategic approach of the Russian Federation when using hybrid influence against the Czech Republic, where the individual areas of specific Russian activities are systematically characterized. The following chapters analyze Russia’s comprehensive cross-domain approach, cyber influence, information operations and, last but not least, intelligence activities, together with political and economic influence.

#### 5.1.1 Comprehensive Cross-Domain Approach

Valery Gerasimov, the Chief of the General Staff of the Russian Federation Armed Forces stated:

*The focus of confrontational methods shifts to the widespread use of political, economic, informational, humanitarian and other non-military measures, which are implemented with the participation of possible public protests. These measures are complemented by covert military measures, including the implementation of information warfare measures and special force actions. The open use of force, often under the guise of peace-making activities and crisis management, only takes place at a certain stage, in principle to achieve the ultimate success in the conflict [1].*

In practice, this statement, together with the experience acquired by the Russian Federation during the Ukrainian crisis, represents the starting points for the Directive on the development of Russian military capabilities by 2020, which indicates a shift:

- 1) From direct destruction to direct influence;
- 2) From direct annihilation of the opponent to its inner decay;
- 3) From a war with weapons and technology to a culture war;
- 4) From a war with conventional forces to specially prepared forces and commercial irregular groupings;
- 5) From the traditional (3D) battleground to information/psychological warfare and war of perceptions;
- 6) From direct clash to contactless war;
- 7) From a superficial and compartmented war to a total war, including the enemy’s internal side and base;
- 8) From a war in the physical environment to a war in the human consciousness and in cyberspace;
- 9) From symmetric to asymmetric warfare by a combination of political, economic, information, technological, and ecological campaigns; and
- 10) From war in a defined period of time to a state of permanent war as the natural condition in national life [2].

Anyway, it is necessary to mention that Russia has tailored its approaches to the particular target. Due to this fact there are differences between theory and real-time actions, especially when the other side responds.

Nevertheless, although the Russian military never openly published something similar to the Phasing Model Construct, it is possible to derive something similar from the literature and the actions in Syria and Ukraine:

- **First Phase:** Non-military asymmetric warfare (encompassing information, moral, psychological, ideological, diplomatic, and economic measures as part of a plan to establish a favorable political, economic, and military setup).
- **Second Phase:** Special operations to mislead political and military leaders by coordinated measures carried out by diplomatic channels, media, and top government and military agencies by leaking false data, orders, directives, and instructions (the so-called leakage).
- **Third Phase:** Intimidation, deceiving, and bribing government and military officers, with the objective of making them abandon their service duties.
- **Fourth Phase:** Destabilizing propaganda to increase discontent among the population, boosted by the arrival of Russian bands of militants, escalating subversion.
- **Fifth Phase:** Establishment of no-fly zones over the country to be attacked, imposition of blockades, and extensive use of private military companies in close cooperation with armed opposition units.
- **Sixth Phase:** Commencement of military action, immediately preceded by large-scale reconnaissance and subversive missions. All types, forms, methods, and forces, including special operations forces, space, radio, radio engineering, electronic, diplomatic, and secret service intelligence, and industrial espionage.
- **Seventh Phase:** Combination of targeted information operations, electronic warfare operations, aerospace operations, continuous air force harassment, combined with the use of high-precision weapons launched from various platforms (long-range artillery, and weapons based on new physical principles, including microwaves, radiation, non-lethal biological weapons).
- **Eighth Phase:** Roll over the remaining points of resistance and destroy surviving enemy units by special operation conducted by reconnaissance units to spot which enemy units have survived and to transmit their coordinates to the attacker's missile and artillery units; fire barrages to annihilate the defender's resisting units by effective advanced weapons; airborne operations to surround points of resistance; and territory mopping-up operations by ground troops. Peacekeeping operations [1].

A very important aspect of waging hybrid warfare presented by the Russian Federation, which follows from the above-mentioned information, is the fact that the open use of force is a further possible final tool of a hybrid campaign. Not only may this tool not always be used, but it may even be undesirable, provided that the objectives can be achieved by other means. Thus, a clear interpretation is offered, namely that the sense of a hybrid campaign in the Russian concept is to achieve set goals while avoiding an open armed conflict. The conceptual and doctrinal approach of the Czech Republic and its NATO allies still shows a certain degree of misunderstanding. NATO's response to this is an emphasis on re-strengthening conventional military capabilities and traditional "D&D" (deterrence and defence). However, this approach creates a somewhat absurd situation, in which NATO deters the Russian Federation from a war that the Russian Federation does not want to wage. Despite this fact, the argument can be made that Russia would have behaved far more aggressively with other border countries if it were not for the NATO.

In the Czech Republic, this approach finds expression in, among other things, the activities of all Russian Intelligence Services (the GRU military intelligence, the SVR civilian intelligence, the FSB internal security service and the Federal Protective Service); in the activities of cyber espionage groups linked to the Russian state power (Turla, Zebrocy, APT28 and others); in pro-Russian activism of proxy actors; in the dissemination of misinformation through proxy actors motivated by the Russian Federation; and in the economic field, e.g., in the efforts to engage in strategically important critical infrastructure projects (completion of Dukovany) [3].

A. Nagorny and V. Shurygin, when analyzing Russia's most important strategic challenges established ways and instruments the West could employ against it. Although they could allegedly be used by the West against Russia, in reality they strongly reflect the Russian asymmetric strategy operationalized in Ukraine:

- 1) Stimulation and support of armed actions by separatist groups with the objective of promoting chaos and territorial disintegration;
- 2) Polarization between the elite and society, resulting in a crisis of values followed by a process of reality orientation to Western values;
- 3) Demoralization of armed forces and the military elite;
- 4) Strategic controlled degradation of the socio-economic situation;
- 5) Stimulation of a socio-political crisis;
- 6) Intensification of simultaneous forms and models of psychological warfare;
- 7) Incitement of mass panic, with the loss of confidence in key government institutions;
- 8) Defamation of political leaders who are not aligned with Russia's interests; and
- 9) Annihilation of possibilities to form coalitions with foreign allies.[4]

### **5.1.2 Cyber Influence**

Cyberspace became an officially recognized operational domain based on a joint decision made by NATO Defence Ministers on June 14, 2016 [5]. Currently, NATO recognizes five operational domains, namely air, land, sea, cyberspace and space. The last two domains named have gained an official character relatively recently, and cyberspace in this respect has overtaken space, which was not recognized until 2019 [6]. The importance of cyberspace was growing for a long time before its official recognition as a new domain, and it would not be a surprise if NATO had taken this step several years earlier. It follows from this fact that the stimulus for this step on the part of NATO was undoubtedly also an assertive way of using cyberspace by the Russian Federation within hybrid operations. One example of such use of offensive cyber tools was, among other things, the attack on energy infrastructure in Ukraine in 2015, which caused the disconnection of 30 substations in the Ivano-Frankivsk region and a power outage that affected up to 80,000 people [7].

The way strategists perceive cyberspace in the Russian Federation is different from the Western concept in many respects. These differences manifest themselves, for example, in the very definition of cyber warfare or in the way the Russian side uses its cyber capabilities. Russian military theorists do not use the term cyber warfare. They do not perceive cyber operations as a separate discipline, but as a subset of information warfare, which in their interpretation includes computer network operations, electronic warfare, psychological operations and information operations. Within information warfare, cyber operations are used, among other things, for "cyber espionage" activities, attacks on critical infrastructure and other ways leading to the achievement of information warfare strategic goals.

The main feature of Russia's offensive cyber operations has so far been the use of the so-called "hacktivists" (people who use "hacking" as a form of expression of civil disobedience in support of political agenda or a social change) and cybercrime syndicates. These groups are then able to provide the state with mainly the following capabilities:

- 1) Organizing Distributed Denial-of-Service (DDoS) attacks;
- 2) Antivirus testing to detect malware;
- 3) Malware "packages" (modify malicious software so that it is not detected by an antivirus);
- 4) Rental of "exploit packs";

- 5) Rental of dedicated servers;
- 6) VPN (providing anonymous access to web resources and data exchange protection);
- 7) Renting out abuse-resistant hosting (hosting that does not respond to complaints about malicious content and, therefore, does not shut down the server);
- 8) Renting out botnets; and
- 9) Evaluation of data on stolen credit cards and the service of verification of this data.

The advantage of using the services of these non-state actors lies primarily in their easy mobilization and anonymity, which makes attribution difficult. However, it is assumed that in the future these tools will be replaced by a more “tailor-made” approach, where the FSB and other government agencies will play a central role. Until 2008 (the war in Georgia), the military use of “cyber operations” was limited only to the areas where there was an overlap with electronic warfare. However, the shortcomings in capabilities identified during this campaign led to the intention to set up a unit within the armed forces responsible for conducting information operations, which would employ hackers, journalists, strategic communication specialists, psychological operation specialists and linguists. In 2013, the Russian Government also announced its intention to create a cyber-unit specialized, among other things, in offensive and defensive cyber operations. However, the current status of these projects is not known [8].

To describe in a comprehensive and systematic way the cyber influence conducted by the Russian Federation against private, public and state objects in the territory of the Czech Republic and abroad, and thus the Czech Republic itself, is complicated to a large extent. One obstacle is the fact that the attribution of such an influence is a purely political responsibility, when it is often not in the state interest to make the attribution publicly. Another obstacle is the very nature (modus operandi) of the Russian cyber influence described in this chapter, the aim of which is to operate below an imaginary threshold, the exceeding of which would allow the unambiguous attribution.

The annual reports of the Security Information Service and the National Cyber and Information Security Agency reveal part of this influence. In its annual report for 2017, the Security Information Service informs about cyber espionage against the Czech Republic, when the information system of the Ministry of Foreign Affairs was compromised. Compromising the MZV e-mail system was taking place at least since the beginning of 2016, when the attackers accessed more than 150 e-mail boxes of employees, copied e-mails, including attachments, and obtained data usable for future attacks on other state institutions. In parallel with this incident, there was also an attack on other e-mail boxes of the same Ministry. These incidents were probably independent of each other and, based on all the findings of the Security Information Service done, it is clear that these were the cyber espionage campaigns of the Turla Group (originally from the Russian FSB) and the Sofacy Group, also known as ATP28 (attributed to the Russian military intelligence service – GRU). The Security Information Service also reported on a wave of spear phishing attacks targeting military diplomats in Europe, when the vector and targets of these attacks were fully consistent with the type of attacks and the areas primarily targeted by the Russian APT28/Sofacy cyber espionage campaign [9]. In the annual report for 2018, the Security Information Service reported on compromised private e-mail accounts owned by the members of the Army of the Czech Republic, which, according to the Czech Information Service findings, is also supported by the Russian APT28/Sofacy cyber espionage campaign. This did not cause the leakage of classified information according to Act No. 412/2005 Coll.; however, the attackers gained access to a number of sensitive personal data that may be misused in the future for further attacks in the form of social engineering, not only against the Armed forces of the Czech Republic members [10]. In its annual report for 2019, the Security Information Service reported on other findings concerning the activities of cyber espionage groups linked to the Russian Federation. In 2019, the Security Information Service took part in the investigation of the attack on the ICT infrastructure of one of the Czech diplomatic missions to an international organization, when the Russian Federation was most likely the attacker again [11].

The report on the state of cyber security in the Czech Republic for 2020, issued by The National Cyber and Information Security Agency, as well as the reports for 2019 and 2018, is not specific in terms of attribution. However, this report confirms that cyber-attacks are on the rise and this trend is expected to continue. The report also confirms that the activities of state-supported actors in cyberspace fall among the most serious threats to cyber security in the Czech Republic [12].

In 2020, there were also a few serious cyber-attacks on, inter alia, the Ministry of Health, Václav Havel Airport, hospitals in Ostrava, Olomouc, the Pardubice and Karlovy Vary region. The Czech newspaper found out that even in these cases, the Russian Federation was behind the attacks, namely with reference to sources close to the investigation and a member of the National Security Council. However, these findings have not been officially confirmed [13].

### **5.1.3 Information Operations**

Information operations are another tool used by the Russian Federation in waging hybrid warfare. Russia's information operations have evolved to create a multiplier effect through many information channels with a view to manipulate, distort, filter, extract and insert information to ensure that the only available sources of information will be those approved by the Russian Government. These channels used include, inter alia, the following:

- 1) Traditional or "alternative" media, through which disinformation spreads;
- 2) Troll campaigns;
- 3) Official government statements;
- 4) Speeches at rallies or demonstrations;
- 5) Offensive videos uploaded to YouTube;
- 6) Sending text messages directly to phones or even; and
- 7) Direct contact of people in the street and oral transmission of the message.

This approach is reflected in the Russian doctrine, which considers information to be an essential element of information operations, regardless of the channel that transmits this information. The goal of the Russian Government is, therefore, to check all information, regardless of the platform, whether it is online or print media or the beliefs of individuals or masses [14].

However, the check of information itself is not enough, and three other factors are needed to ensure a successful "propaganda campaign". These factors correspond to the intention to create a multiplier effect through the diversity of sources that promote a given narrative. The first factor is the fact that more sources repeating the same message make a more convincing impression than one and, moreover, they provide different points of view, which leads to a more significant consideration on the part of the information recipient. The second factor is the fact that the amount of resources that convey the information provides this narrative with validity, which can strengthen the perception of the credibility and reliability of information regardless of the quality of the arguments. This fact was confirmed by a study conducted in 2018 at Yale University, which revealed that the key in people's decisions, whether to believe in something or not, was acquaintance. This study shows that the more times a person has seen a certain headline or a similar one, the more likely he or she has believed that it is a fact, regardless of whether the information is false. The third factor is the fact that if the information is disseminated from the group, the member of which is the recipient of information or with which he identifies, the probability of receiving this message also increases significantly [14]. However, the goal of Russia's information operations may not always be to enforce its own narrative. In the past, the so-called "overwhelming the information environment" also became a commonly used procedure. The purpose in this case is to overwhelm the information space with a lot of different information in order to blur the line between the truth and a lie. In the case of achieving the set goal

using this method, society gets the impression “God knows how it was” in the context of a specific event and the unification of society is effectively paralyzed, for example, as concerns the support of specific government actions.

The Czech Republic has witnessed many examples of Russian information operations in recent years. A typical example of a Russian information (influence) operation (not only in terms of implementation, but also in terms of targeting NATO’s unity and strengthening) there was an effort around 2008 to prevent the establishment of a radar base in Brdy as part of the US anti-missile defence in Europe [15]. Examples from recent years include, inter alia, the activities in connection with the Ukrainian and Syrian conflicts, responses to the debate, and finally the decision to remove the statue of Marshal Konev from Prague 6 and the Russian Sputnik V vaccine promotion.

To better understand the Russian information influence in the Czech Republic, the following paragraphs describe in detail the specific information influence in connection with the Government announcement of April 17, 2021. There is a reasonable suspicion that the explosion of ammunition depots in Vrbetice<sup>1</sup> may have been due to the activities of the Russia’s GRU intelligence service.

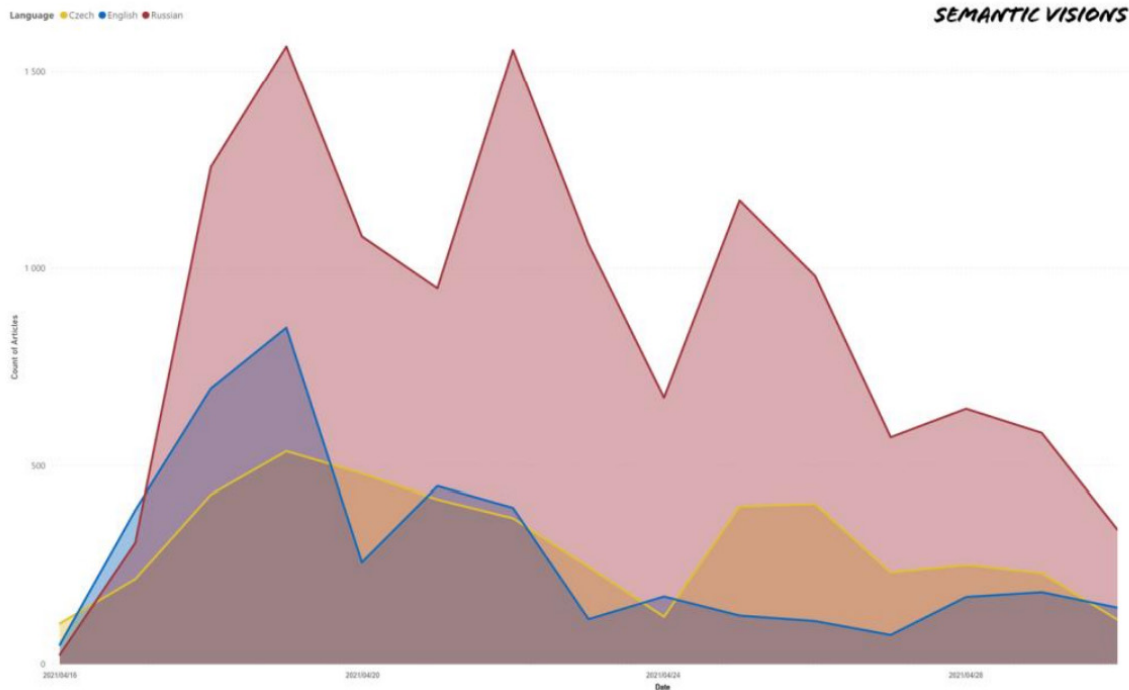
The main points in the development of the pro-Kremlin disinformation campaign aimed at the reaction of Czech disinformation sources as well as the domestic Russian media in the period under review from April 17, 2021 to May 4, 2021 (Figure 5-1), were the following:

- The Czech disinformation media persistently promotes a pro-Kremlin interpretation of the GRU scandal in the spirit of traditional pro-Kremlin and anti-Western propaganda. These media often reinforce Russian disinformation narratives and official statements by the Kremlin and support domestic political actors who hold populist, pro-Kremlin positions, such as the far-right SPD, the Communist Party (KSCM) and Czech President Milos Zeman, notorious for his friendly attitude towards Vladimir Putin. However, despite their pro-Kremlin orientation, most of these sites do not have obvious ties to the Russian state and do not create content in coordination with the Russian media. Their main drivers are profit (i.e., advertising revenues) and social influence.
- Specifically, the Czech disinformation media tried to ridicule and discredit the official government description of what happened in Vrbetice, especially evidence of Russia’s involvement. For this purpose, they offered several alternative explanations as well as conspiracy theories about motivating the government to point the finger at the GRU, which suggests that this is a trick how to escalate the conflict between Russia and the West provoked by the United States. Other key narratives focused on casting doubt on announcement timing and attacking the competencies and credibility of the Czech security services.
- Russia’s disinformation response to the revelation of the GRU role in Vrbetice was immediate and followed the same plan as in other cases, when Russian criminal activity, such as the annexation of Crimea and the poisoning of Skripal, was discovered. Russian officials and the pro-government media deny any Russian involvement in the blast and reject the reaction of the Czech Government as an attempt to gain points in Washington’s “war of sanctions.” The dominant narratives in the Russian media alternatively attribute the scandal to American puppetry in the Czech Republic and the alleged “Russophobia” of the Czech authorities. In this respect, there is a clear difference in the negative information about the government of Prime Minister Babis, which ordered the expulsion of Russian diplomats and considers the GRU attack to be an act of state terrorism, and positive information about President Zeman, who falsely claimed that there was no evidence of the Russian Intelligence Service involved in the blast.

---

<sup>1</sup> In 2014, two explosions of ammunition depots occurred in Vrbetice area. Two people were killed. According to the intelligence service and police, two agents from GRU were involved in the explosions, with the motivation of disrupting weapons supplies to Ukraine.

- Pro-Kremlin disinformation efforts in Russia as well as in the Czech Republic were strongly supported by President Zeman in his speech on April 25, in which he denied the official attitude of the Czech Government to the GRU involvement and instead he stated that the explosions had been probably caused by mishandling ammunition. The speech was strongly promoted by the Russian-language media, which praised Zeman for not succumbing to pressure from the United States. Czech disinformation websites also supported it as the “voice of reason” in the middle of all “Russophobic hysteria” [16].



**Figure 5-1: The Total Number of Articles about Vrbotice Published Daily in the Observed Period in Czech (Yellow), English (Blue) and Russian (Red). (Source: Semantic Visions.)**

#### **5.1.4 The Operation of Intelligence Services and Political and Economic Influence**

The Security Information Service and Military Intelligence deal with the operations of Russian Intelligence Services in the Czech Republic within their counterintelligence activities. The possibility of obtaining more detailed information for the public is very limited with regard to the naturally confidential character of this information. The obligation of the above-mentioned entities is to give information only to the following addressees (President of the Republic, Prime Minister, relevant members of the Government, state authorities and police authorities). As a matter of fact, the public can learn about the operation of Russian Intelligence Services on the Czech territory only from the annual reports of these intelligence services. The Security Information Service has long been more open in communicating findings concerning the operations of the Russian Intelligence Services.

The constant of the Security Information Service annual reports for the last 10 years (annual reports from 2010 to 2019) is that they identify the Russian Intelligence Services as the most active on our territory in terms of the frequency and intensity of activities; there are a number of intelligence officers operating under different cover. The disproportion in the numbers of Czech and Russian diplomatic missions has long been a significant limiting factor for the Czech Republic and its security interests in dealing with the situations; there are a lot of

cases when Russian intelligence officers under diplomatic cover carried out activities incompatible with the job description of a diplomat. This fact was not resolved until 2021, when equal representation was established in response to the revelation of the background of the Vrbetice explosions [17].

Based on the information published in the annual reports of the Security Information Service, the following points can be identified as key areas of interest for the operation of Russian Intelligence Services in the Czech Republic:

- 1) Efforts to cultivate the Russian compatriot community in the Czech Republic.
- 2) Strengthening information and influence capacities aimed at the Czech economy and energy industry.
- 3) Strengthening the influence of the so-called gray zone on the state power and self-government structures.
- 4) Long-term building of propaganda structures, the aim of which is to promote and protect Russian economic and political interests at the expense of the interests of the Czech Republic and thus NATO and the EU.

The fact that part of the Russian diaspora in the Czech Republic holds a negative attitude towards the efforts of the directive management by the Ministry of Foreign Affairs of the Russian Federation can be perceived as positive news. In the period around 2010, special attention was paid to the Russian-speaking community, especially to the representatives of the Caucasian peoples. This fact resulted mainly from the then security situation in the Caucasus region. As for the cooperating part of the diaspora, the priorities in striving for improvement changed over the years from 2010 to 2019. One of the tasks of compatriot organizations identified by the Security information Service in 2010 was to help Russia's scientific and technical development. Efforts to marginalize anti-Kremlin-oriented compatriot entities and to increase the influence of those compatriot entities that sympathize with the current political representation of the Russian Federation can be considered a long-lasting effort towards the Russian-speaking community in the Czech Republic. It is also worth mentioning the contacts of Russian intelligence officers to persons whose past is associated with Russian-speaking organized criminal structures and their activities in the territory of the Czech Republic [17].

Within strengthening the influence of the so-called gray zone, the influence of non-elected entities without political and official responsibility spread in the period under review that promoted their influence at all levels of state and local government, e.g., lobbyists, lobbying, consultancy or law firms, interest and networking groups. Russian influence also spread through Russian acquisitions of Czech private business companies and Russian lines leading to the environment of Czech cases related to corruption or other illegal activities. The principle of the problem rests in the fact that Russian investors (often represented by former members of the Russian Intelligence Services) hidden behind Czech stooges or offshore companies, controlled a Czech company that wins or seeks government contracts (including power department contracts) and, moreover, they employed managers who in the past had been involved in media or police cases within corrupt practices. The Security Information Service also noted the efforts of Russian intelligence officers to build links and cultivate an influence base close to the politicians who exercise influence on the development in the areas of interest of the Russian Federation [17].

Apart from an abstract description of the modus operandi of the Russian services, both the Security Information Service and the Czech media reported on several specific incidents related to the activities of the Russian Intelligence Services. These publicly known manifestations include, inter alia, open assistance to specific Czech citizens as well as hidden assistance in traveling to the problem areas of Ukraine [18]. The manifestation of this trend could be observed by the public in April 2021, when people suspected of organizing trips of Czech citizens to Ukraine were arrested for fighting for pro-Russian separatists [19]. In its annual report for 2018, the Security Information Service also reported on a joint action with a partner intelligence service, on the basis of which the activities of the Russian FSB (Federal Security Service) were revealed, which was secretly building ICT infrastructure in the territory of the Czech Republic.



This infrastructure was part of a larger system that could be used for classified cyber and information operations of the FSB within the local and global scope. In cooperation with the Police of the Czech Republic, this network was broken and thus prevented the activities of the FSB against the interests of the Czech Republic or our allies [10]. The case of Robert Rachardžo, who successfully obtained information from the environment of the Armed forces of the Czech Republic Headquarters, is also interesting [20]. The “Vrbetice incident” remains the most publicly known activity of the Russian Intelligence Services.

## **5.2 PROPOSALS, RECOMMENDATIONS AND IMPLICATIONS**

In accordance with the analysis of the strategic approach of the Russian Federation in using hybrid influence, basic proposals and recommendations for the implementation of measures to increase the resilience against Russian hybrid threats were set out within the moderated discussions of the panel of experts.

### **5.2.1 Proposals and Recommendations in the Construction and Strengthening of Resilience in the Czech Republic**

In an effort to achieve a higher resilience of the Czech Republic against hybrid threats, responsible representatives are exposed to many challenges. To effectively counter this way of conducting a conflict requires not only a supra-ministerial but even a whole-of-society approach. In its recent history, the Czech Republic has not yet been forced to face an external security threat, which cannot be “arrested, shot or banned.” In developing a national approach, it is an indisputable necessity to move away from the traditional modus operandi of the state administration and to cross the invisible but strongly perceived boundary between the public and private sectors. This holistic approach can range from the school education system through the involvement of key representatives of the national economy to the creation of new capabilities of the armed forces.

#### **5.2.1.1 Coordination**

The very nature of the type of hybrid influence determines that the prevention, effective mapping of this influence and the subsequent response to it cannot be a matter under the responsibility of only one ministry, but it requires a coordinated supra-ministerial approach. Within the international position of the Czech Republic, it is then a natural necessity to further synchronize this national approach with our allies in the EU and NATO. The following proposed solutions in the Czech Republic would, among other things, make the supra-ministerial coordination of countering hybrid influence more effective:

- 1) Strengthening the role of the Expert Working Group on Hybrid Threats of the National Security Council, in particular by extending this Expert Working Group to other relevant ministries and the possibility of setting up coordination and analytical subgroups for information sharing and possible detection of hybrid influence. Within this Expert Working Group, to set up a function of a coordinator of the agenda to counter hybrid threats, who would be subordinated to the National Security Adviser.
- 2) To establish a system of strategic communication of the state, including a mechanism for systematic coordination of relevant actors.
- 3) To create a national network of selected experts in the field of countering hybrid influence from a number of experts from the academic, research, non-governmental and private spheres for the purpose of implementing research, awareness-raising and other projects.
- 4) To strengthen international cooperation in confronting hybrid influence with the allies of NATO and the EU.
- 5) To use vulnerability mapping tools in cooperation with NATO and the EU and to establish a single mechanism at the national level for conducting regular mapping of critical infrastructure vulnerabilities to hybrid influence.

### **5.2.1.2 Updating the Conceptual, Doctrinal and Legislative Framework**

Adapting the system to this security threat also brings the need to update the existing conceptual, doctrinal and legislative framework. These are, inter alia, the following steps:

- 1) To create a concept of an exercise focused on facing hybrid influence.
- 2) To take into account the issues of countering hybrid influence within updating the National Defence Plan of the Czech Republic and the Report on the Czech Republic Defence.
- 3) To take into account hybrid influence and to identify related threats within updating the Threat Analysis for the Czech Republic.
- 4) To use the list prepared by NATO and create a framework of indicators that can contribute to the detection of hybrid influence in the Czech Republic.
- 5) To create a set of possible reactions to the detected hybrid influence in the Czech Republic, including the possibilities of attribution.
- 6) To elaborate and submit proposals for changes in legislation to the Government to strengthen the capabilities of the Czech Republic to face disinformation.

### **5.2.1.3 Strengthening the Resilience of Society, the State and Critical Infrastructure**

In the area of strengthening the resilience of society, the state and critical infrastructure, the development is taking place mainly through education policies and activities. Media literacy and critical thinking are gradually being included in the framework educational programs with the aim of increasing social resilience already in primary and secondary schools. The intelligence services and the Ministry of the Interior also play a role in this area, providing regular training for government employees in order to systematically increase the resilience of the state administration. The topic of hybrid influence is also taken into account in the educational programs of the Diplomatic Academy of the Ministry of Foreign Affairs in order to increase the awareness and readiness of the diplomatic corps. At the request of Charles University, the “Counter Foreign Interference Manual for the Czech Academic Sector” was also elaborated and published. It describes general resilience-building measures against foreign interference on an institutional level and presents the most common interference techniques foreign powers use against individuals. Further strengthening of resilience can be achieved, inter alia, as follows:

- 1) To raise awareness of foreign investment screening in the private and public sectors, including foreign partners, by developing a set of recommendations on foreign investment screening for the private sector and through seminars, internal training and communication campaigns.
- 2) By processing the analysis of the critical infrastructure resilience to hybrid influence and by implementing measures resulting from it.
- 3) By setting transparency in the financing of non-profit organizations, especially those that deal with key issues related to the security and foreign policy interests of the state.
- 4) By integrating media education into the strategies and framework educational programs of primary and secondary schools, by methodical support of kindergarten, primary and secondary school teachers in the field of civics and media literacy, and by supporting the integration of media education into the education of students of pedagogical faculties.
- 5) By submitting a proposal related to extending the current training system to the Government to strengthen the resilience against the influence of foreign power to, if possible, mandatory training for state officials and recommended training for local government officials, including the creation of an e-learning platform and training of trainers.

- 6) By creating a “National Defence Course” inspired by the Finnish Security System. This course would be attended by government-nominated organizations, government officials, soldiers, representatives of political parties, media, scientific and cultural organizations, non-governmental organizations and private companies working in security-relevant positions, including e.g., the heads of the largest Czech companies. The participants would get acquainted with the overall functioning of the security system, national defence and foreign policy as well as the role of each of its components.

#### **5.2.1.4 Proactive Approach**

The aim of the proposed proactive approach (in addition to manifestations of hybrid influence and enhancement of resilience) is not only to limit the countering of hybrid threats and combating the manifestations of this effect, but also to actively discourage the adversary from this type of action. The proactive approach on the part of the Czech Republic could manifest itself, among other things, as follows:

- 1) By involving the issues of hybrid influence in exercises, by participation and regular evaluation of exercises with the elements in dealing with hybrid influence, including international exercises in cooperation with NATO and the EU.
- 2) By discouraging the adversary from using the tools of hybrid influence in the form of proactive defence (reactive mode), based on unambiguous attribution to perform offensive cyber operations and information operations.
- 3) By consistently combating criminal activity on the Internet, e.g., through the use of Section 357 of the Criminal Code on the dissemination of alarm messages.
- 4) By cooperation with the private sector – to positively motivate private entities in the restriction of advertising and thus the financing of demonstrably disinformation websites.

In this case, point 2 seems to be controversial and politically sensitive. However, from the military point of view, when the defender does not only want to have a secure system with the ability to quickly repair the damage, but he wants to directly deter the enemy from attacks, this procedure seems to be necessary. The actual offensive action or the threat of such an action can lead to a situation when the attacker loses significantly on his activities and is willing to give up his hostile activities.

#### **5.2.2 Proposals and Recommendations for the Armed Forces of the Czech Republic**

Proposals and recommendations for the construction and strengthening of the Czech Republic’s resilience to hybrid influence can also be applied in the context of the Armed forces of the Czech Republic and thus to achieve greater resilience of the armed forces to hybrid threats. It is especially important for the Armed forces of the Czech Republic to accept and adapt to the fact that in the context of the Russian threat, the paradigm has changed, which is now moving the area of rivalry with the Russian Federation to the level of information warfare. Nevertheless, this fact does not reduce the need for conventional capabilities as building and maintaining them in cooperation with NATO has a deterrent effect that ensures that the enemy’s self-confidence does not grow to the point when he believes in his victory in conventional conflict.

The proposed capabilities and measures apply, in particular, to:

- Strengthening personnel security;
- The training of military personnel, internal ideological and motivational coherence;
- Increasing the resilience of soldiers – training, education, warrior ethos;
- Achieving the independence of the Armed forces of the Czech Republic from Russian equipment and spare parts;
- Conducting offensive information and cyberspace operations; and
- Monitoring and better knowledge of the enemy.

Strengthening personnel security and training of soldiers are in some points connected aspects, when one part without the other cannot achieve the desired effect. The personnel security of the Armed forces of the Czech Republic members (hereinafter referred to as “persec”) could be strengthened in the context of hybrid influence by extending the principles already used, for example, in members of special forces and Military Intelligence to a wider range of members of the Armed forces of the Czech Republic. This would limit in particular the publication of the faces and names of soldiers in the media or on social networks, with the exception of the minimum necessary for the presentation of the Armed forces of the Czech Republic to the public. This step would significantly limit the adversary’s ability to “target” hybrid action on specific individuals. However, this step does not have the potential to achieve its goal without soldiers being intensively educated in the form of “countering foreign interference training”. This training would teach soldiers to recognize the attempts of foreign power to establish cooperation, to influence or to obtain information on safe behavior in all domains with an emphasis on the cyber environment. The mapping of soldiers’ views in terms of ideological and moral coherence is equally important. In the context of behavior in the cyber environment, it is worth considering and applying a “Code of Conduct for Soldiers on the Internet”, which would appeal against non-disclosure of affiliation to the Armed forces of the Czech Republic in all possible forms, such as social networks and would regulate the content shared by soldiers. The fact that reducing the Armed forces of the Czech Republic ‘s dependence on Russian equipment and spare parts for it is, to a certain extent, an ongoing process that can be seen as positive news. One of the important steps in this respect has been the decision to replace the Mi-35/24V attack helicopters with the UH-1Y Venom and AH-1Z Viper. This trend should continue with the modernization of the mechanized brigade, e.g., by purchasing new Infantry Fighting Vehicles (IFVs) instead of BVP-2 and other acquisitions replacing the equipment of the Russian origin. However, it would be a fatal mistake in this modernization campaign to lose the ability to work with the equipment of Russian origin; this would lead to a weakening of the level of understanding the enemy and the loss of a certain advantage of the states of the former Eastern bloc within NATO.

It is probable and historical examples verify this statement that in the event of an attack or a repeated attack on their own territories, the Czech Republic and NATO would not limit themselves in response to mere defence; they would not accept the fact that an invasion is taking place, but, on the contrary, such an action would be responded to by their own offensive, the task of which would be to end this threat. A special fact is a piece of knowledge that although the Czech Republic is repeatedly attacked by information warfare means, the public debate is mostly kept within the bounds of building and strengthening its own resilience. Part of the solution proposed is a reassessment of its own attitude and building offensive capabilities in the field of information and cyber operations. If one of the first points of the adversary’s actions is to find a dividing line in society, in which he wants to operate, it can be stated that authoritarian regimes are by their nature, including greater need to maintain continuity of power in the state, significantly more sensitive to this type of action. The utilization of the opponent’s attack mechanisms against himself, together with the increasing complexity of successful operations resulting from our own resilience, can be an important step in discouraging the opponent from continuing his activities. A prerequisite for the Armed forces of the Czech Republic to be able to carry out such operations is, inter alia, intensive monitoring and better knowledge of the enemy and the resulting accurate identification of his strengths and weaknesses.

### 5.3 REFERENCES

- [1] Čekínov, S.Č., Bogdanov S.A. O povaze a významu války nové generace. [“The Nature and Content of a New-Generation War.”] *Vojenská mysl*, 10, 2013, pp. 13-24. <https://www.vojenskerozhledy.cz/kategorie/novy-rusky-zpusob-vedeni-valky-a-lotyssko>
- [2] Bērziņš, J. “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy.” *Policy Paper 2*, 2014, pp. 2002-2014.

- [3] Czech Security Information Service, BIS. Výroční zpráva Bezpečnostní informační služby za rok 2019. [“Annual Report of the Security Information Service for 2019.” Prague. <https://www.bis.cz/public/site/bis.cz/content/vyrocnizpravy/2019-vz-cz.pdf> Accessed 10 October 2021.
- [4] Nogurny, A. and Shurygin, V. (eds.). Defense Reform as an Integral Part of a Security Conception for the Russian Federation: A Systemic and Dynamic Evaluation. Moscow, Izborsky Club, 2013.
- [5] North Atlantic Treaty Organization. “Cyber Defence.” 2021. [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm) Accessed 10 October 2021.
- [6] North Atlantic Treaty Organization. “NATO’s Approach to Space.” 2021. [https://www.nato.int/cps/en/natohq/topics\\_175419.htm](https://www.nato.int/cps/en/natohq/topics_175419.htm) Accessed 10 October 2021.
- [7] Boháček, P. Kybernetická válka je další formou rusko-ukrajinského konfliktu. [“Cyber Warfare Is Another Form of Russian-Ukrainian Conflict.”] Natoaktual.cz. 18 April 2016. [https://www.natoaktual.cz/analyzy-a-komentare/kyberneticka-valka-je-dalsi-formou-rusko-ukrajinskeho-konfliktu.A160418\\_151213\\_na\\_analyzy\\_m02](https://www.natoaktual.cz/analyzy-a-komentare/kyberneticka-valka-je-dalsi-formou-rusko-ukrajinskeho-konfliktu.A160418_151213_na_analyzy_m02) Accessed 11 October 2021.
- [8] Connell, M., Vogler, S. “Russia’s Approach to Cyber Warfare (1Rev).” Center for Naval Analyses, Arlington, United States, 2017.
- [9] Czech Security Information Service, BIS. Výroční zpráva Bezpečnostní informační služby za rok 2017. [“Annual Report of the Security Information Service for 2017.”] Prague, 2018. <https://www.bis.cz/public/site/bis.cz/content/vyrocnizpravy/2017-vz-cz.pdf>
- [10] Czech Security Information Service, BIS: Výroční zpráva Bezpečnostní informační služby za rok 2018 [“Annual Report of the Security Information Service for 2018) Prague, 2019. <https://www.bis.cz/public/site/bis.cz/content/vyrocnizpravy/2018-vz-cz.pdf.pdf>
- [11] Czech Security Information Service, BIS. Výroční zpráva Bezpečnostní informační služby za rok 2019 [“Annual Report of the Security Information Service for 2019.] Prague, 2020. <https://www.bis.cz/public/site/bis.cz/content/vyrocnizpravy/2019-vz-cz.pdf>
- [12] The National Cyber and Information Security Agency, NÚKIB. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020. [“The Report on the State of Cyber Security in the Czech Republic for 2020.”] Prague, NÚKIB, 2021. [https://www.nukib.cz/download/publikace/zpravy\\_o\\_stavu/Zprava\\_o\\_stavu\\_KB\\_2020\\_verze\\_pro\\_tisk.pdf](https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020_verze_pro_tisk.pdf)
- [13] Czech News Agency, LN, ČTK, LN. stopy kyberútoků na české nemocnice vedou do Ruska. Je to provokace, tvrdí Moskva. [“Traces of Cyber-Attacks on Czech Hospitals Lead to Russia. It’s a Provocation, Moscow Says.”] Aktuálně.cz, 20 April 2020. <https://zpravy.aktualne.cz/domaci/stopy-kyberutoku-na-ceske-nemocnice-vedou-do-ruska/r~aa756b66831211eab0f60cc47ab5f122/> Accessed 11 October 2021.
- [14] Morrison, S. “Russian Information Operations.” Unpublished PhD Thesis, Swinburn University of Technology, Melbourne. March – July 2021. [https://researchbank.swinburne.edu.au/file/2ce9bdba-af2e-4638-9758-1f129a237e79/1/Sarah\\_Morrison\\_Thesis.pdf](https://researchbank.swinburne.edu.au/file/2ce9bdba-af2e-4638-9758-1f129a237e79/1/Sarah_Morrison_Thesis.pdf)
- [15] Dodge, M. “Russia’s Influence Operations in the Czech Republic During the Radar Debate.” Comparative Strategy, 39(2), 2020, pp. 162-170.

- [16] Semantic Visions. “Report: Pro-Kremlin Disinformation about GRU Terrorist Attack in the Czech Republic.” 4 May 2021.
- [17] Czech Security Information Service, BIS. Výroční zpráva Bezpečnostní informační služby za roky 2010 – 2019. [“Annual Report of the Security Information Service for 2010 – 2019.”] Prague. <https://www.bis.cz/public/site/bis.cz/content/vyrocní-zpravy> Accessed 10 October 2021.
- [18] Czech Security Information Service, BIS: Výroční zpráva Bezpečnostní informační služby za rok 2016. [“Annual Report of the Security Information Service for 2016.”]. Prague. <https://www.bis.cz/public/site/bis.cz/content/vyrocní-zpravy/2016-vz-cz.pdf> Accessed 10 October 2021.
- [19] Valášek, L. Kundra. O. and Respekt. NCOZ: National Center against Organized Crime, NCOZ při rozsáhlém zátahu zatýkala členy polovojenských jednotek napojené na Rusy. [“The NCOZ Arrested Members of Paramilitary Units Attached to the Russians During the Extensive Raid.”]. Aktuálně.cz, 21 April 2021. <https://zpravy.aktualne.cz/domaci/ncoz-pri-rozsahlem-zatahu-zatykala-cleny-polovojenskych-jedn/r~544007fca21911ebaedf0cc47ab5f122/> Accessed 18 October 2021.
- [20] Gazdík, J. Špion v armádě byl špičkou tajných služeb, teď se po něm slehla zem. [“The Spy in the Army Was a Top Agent of the Secret Service, Now he Has Disappeared Without Trace.”]. Alza.cz, 2 February 2011. [https://www.idnes.cz/zpravy/domaci/spion-v-armade-byl-spickou-tajnych-sluzeb-tese-po-nem-slehla-zem.A110202\\_152821\\_domaci\\_abr](https://www.idnes.cz/zpravy/domaci/spion-v-armade-byl-spickou-tajnych-sluzeb-tese-po-nem-slehla-zem.A110202_152821_domaci_abr) Accessed 18 October 2021.

## Chapter 6 – RUSSIA’S INFLUENCE OPERATIONS IN THE BALTIC STATES

**Jānis Bērziņš**

National Defence Academy of Latvia  
LATVIA

### 6.1 INTRODUCTION

After the events in Crimea and Eastern Ukraine, a prevailing viewpoint among think-tankers, policymakers, and certain scholars emerged, positing that the Baltics would likely be the next target of Russian military action. This prevailing belief is rooted in several assumptions. Firstly, it is presupposed that Russian President Vladimir Putin seeks to revive the Soviet Union. Secondly, the invasion and annexation of the Baltic States are perceived as necessary steps toward achieving this objective. Thirdly, the Russian-speaking population in the Baltics is deemed easily exploitable to support subversive operations similar to those witnessed in Crimea. Operationally, such endeavors were anticipated to be executed through the implementation of ostensible Russian Hybrid Warfare tactics, purportedly aligned with the alleged Gerasimov Doctrine.<sup>1</sup>

However, a significant concern with this assumption lies in its projection of distorted strategic objectives and military instruments to be employed by Russia, which predominantly derive from a narrative propagated by Western actors. Essentially, this perspective disregards Russia’s distinct strategic culture and operational code. While it would be inaccurate to claim that Russia holds no interest in the Baltic Countries, the reality is quite the contrary. The Baltic States continuously experience non-kinetic assaults, utilizing both non-military and military instruments. These encompass psychological, informational, and influential operations, including the financing of pseudo-non-governmental organizations to achieve political goals, disinformation campaigns, and displays of military strength in close proximity to the Baltic States’ borders. Nonetheless, there are currently no indications that Russia intends to engage in a Crimea-like operation to annex the Baltic States.

The Russian strategy concerning the Baltic States is multifaceted and influenced by various factors. Firstly, the Baltic States are considered integral to the West, and as such, their inclusion forms a vital component of Russia’s overarching grand strategy vis-à-vis the West. Secondly, the Baltic Countries’ attainment of independence has resulted in a loss of strategic depth for Russia, given that the NATO border now lies a mere 160 kilometers from Saint Petersburg. Thirdly, the presence of a substantial Russian-speaking population in Estonia and Latvia necessitates consideration. While Russia does not categorize the Baltic Countries as part of the Russian World (Ruskiy Mir), the same cannot be said for their Russian-speaking inhabitants. Russia perceives an obligation to safeguard the interests and preserve the Russian national and cultural identity of compatriots residing abroad [2]. This stance, however, clashes directly with the process of Westernization experienced by the Russian-speaking population in the Baltic Countries. Consequently, Russia’s leverage in the region is diminished as the Russian-speaking community could be exploited as a means of exerting political pressure and engaging in destabilization and influence operations.

This chapter undertakes an analysis of Russia’s non-kinetic warfare, specifically focusing on influence, psychological, and informational operations in Latvia. It asserts that since approximately 2017, the emphasis has shifted toward undermining Western civilization and values, rather than relying solely on pro-Russian

---

<sup>1</sup> The Russians have their own concepts, based on their own military thought. They use the term Hybrid Warfare to refer to the allegedly American and NATO strategy of creating color revolutions as destabilization operations in targeted countries. The Russians refer to their own way of warfare as “New Generation Warfare.” For an analysis of the Russian way of warfare see Bērziņš [1].

narratives and agents of influence. The aim is to exploit inherent systemic vulnerabilities stemming from Latvia's political, economic, and social models, while propagating a fallacious narrative suggesting the decadence of both the West and Latvia itself.

## **6.2 RUSSIA AND THE BALTIC STATES: FINLANDIZATION**

The Baltic Countries rightly perceive the Soviet period as the result of compelled and illicit occupation, while their attainment of independence from the Soviet Union in 1991 is regarded as the reinstatement of the pre-World War II republics. In contrast, Russia perceives the Baltics as recently emancipated states that emerged from the former Soviet Republics of Estonia, Latvia, and Lithuania [3]. Nevertheless, Moscow concedes the historically intricate and contentious nature of the relations between the Baltic States and Russia, which stem from deep-seated disparities in culture, religion, and history, compounded by contemporary predicaments and tensions [4].

While the strategic objectives of occupation and annexation do not presently align with Moscow's immediate ambitions, this does not imply a lack of interest on the part of Russia in the Baltic Countries. On the contrary, Russia asserts its inherent entitlement to a sphere of influence, commonly referred to as the "near abroad," which encompasses the post-Soviet expanse. Given the resolute alignment of the Baltic States with the Western bloc, Russia's foremost objective appears to be the perpetuation and, potentially, expansion of its influence within the region, with the ultimate aim of effectuating a condition of "finlandization" [4].

The term "finlandization" originated from the foreign policy adopted by Finland, which sought to accommodate the interests of the Soviet Union in Northern Europe, while concurrently upholding a stance of non-alignment and preserving democratic principles. In essence, "finlandization" entails the strategic deployment of realpolitik to safeguard national values.

To substantiate the prospective finlandization of the Baltic States, proponents from Russia predominantly rely on economic arguments. It is posited that despite their unwavering membership in NATO and the EU, the current economic and social indicators, pace of macroeconomic advancement, and demographic trends within the Baltic Countries portend a likelihood of depopulation by the middle of the current century. To address this perceived challenge, the proposed solution advocates the preservation of NATO membership status quo, while simultaneously upholding EU membership, in conjunction with the pursuit of "restorative (sic) Eurasian integration" [5].

Thus, the underlying strategic objective, consonant with the principles espoused by Clausewitz, is fundamentally rooted in political considerations. It seeks to gradually shift the Baltic States away from the sphere of Western influence and reintegrate them into Russia's near abroad, without recourse to overt military aggression, annexation, or outright occupation of these sovereign entities. Rather, the envisaged trajectory entails an indirect approach, leveraging the democratic processes inherent to these states as a potent instrument. The strategic blueprint delineated by Russia comprises a comprehensive array of nine key points [6]:

- 1) The stimulation and support of armed actions by separatist groups with the objective of promoting chaos and territorial disintegration.
- 2) Polarization between the elite and society, resulting in a crisis of values followed by a process of reality-orientation to Western values.
- 3) Demoralization of the armed forces and military elite.
- 4) Strategic controlled degradation of the socio-economic situation.
- 5) Stimulation of a socio-political crisis.



- 6) Intensification of simultaneous forms and models of psychological warfare.
- 7) Incitement of mass panic, with the loss of confidence in key government institutions.
- 8) Defamation of political leaders who are not aligned with Russia's interests.
- 9) Annihilation of opportunities to form coalitions with foreign allies.

The efficacy of these influence operations is inextricably intertwined with the presence of susceptible vulnerabilities within the targeted society. Thus, the effectiveness of such operations hinges upon the existence of exploitable vulnerabilities that dovetail with underlying trends. Consequently, the strategic design seeks to exploit inherent weaknesses germane to the subject of attack. Given that the primary objective remains deeply entrenched in the political domain, influence operations explicitly revolve around the identification of key target audiences within the population, a meticulous profiling of their behaviors (both current and dormant), and the formulation of influence pathways that stimulate or mitigate desired behavioral outcomes.

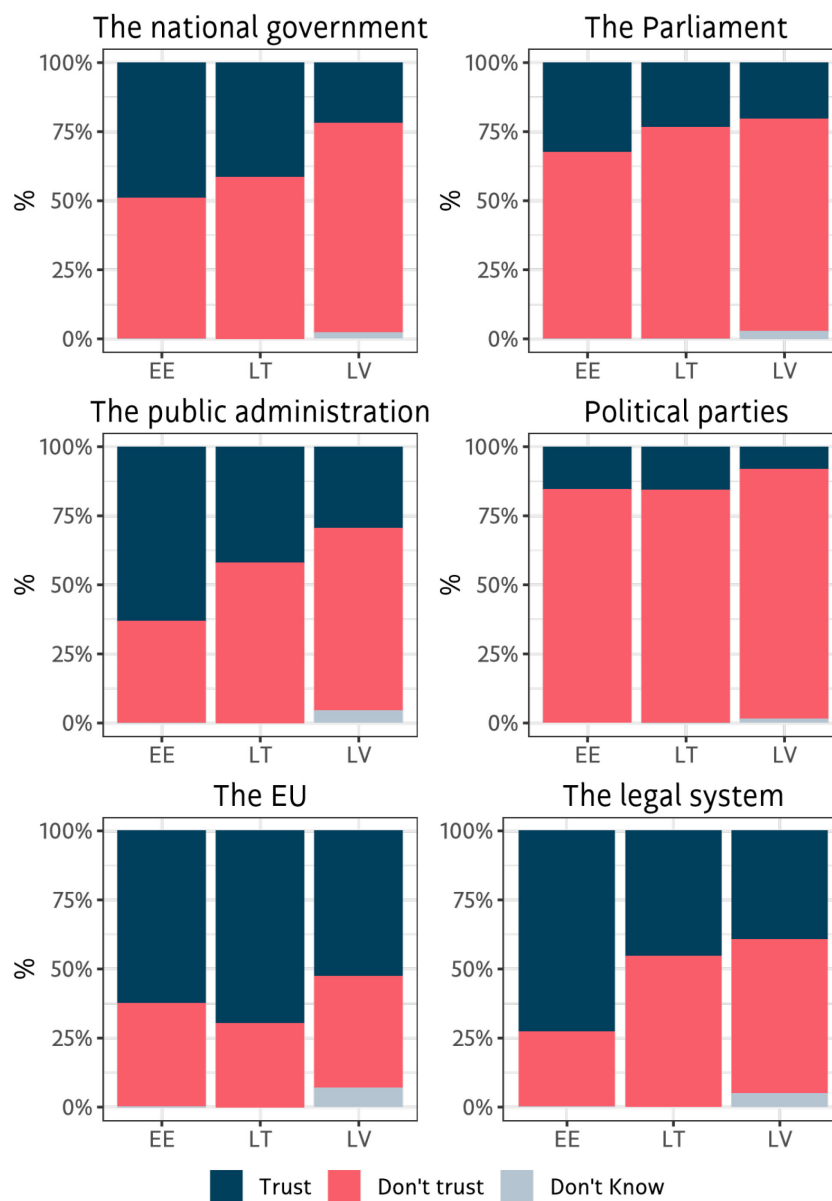
Given the prevailing resistance evinced by the Baltic Countries' populace vis-à-vis any concerted effort to forge closer ties with Russia, the narrative being strategically deployed does not overtly espouse pro-Russian or pro-Eurasian sentiments. Instead, the central tenet revolves around convincing the population that their present alignment with the West, democratic political models, NATO and EU membership engenders impediments that curtail their complete developmental potential. Moreover, the narrative endeavors to portray the innate moral values characteristic of the Baltic States' populace as inherently distinct from Western values, while ostensibly aligning these values with the specific traditional values that Russia espouses. The intended outcome manifests in the democratic election of populist, anti-NATO, anti-European Union, and anti-West political figures, thereby engendering a natural, organic realignment with Russia.

The efficacious implementation of these methods hinges significantly on the level of "exit" exhibited within a given country. The theoretical construct developed by A. Hirschman, comprising voice, exit, and loyalty, furnishes valuable insights into this phenomenon. Dissatisfaction finds expression through voice, involving the direct articulation of grievances, or through exit, typically borne out of the conviction that voicing concerns will yield no tangible outcomes. The resultant corollary posits that heightened voice engenders heightened loyalty, whereas an intensified propensity for exit diminishes loyalty. While exit manifests as a rational choice within the purview of economics, aligning with the principles of market mechanisms, in the realm of politics, exit is emblematic of regressive trends, given that voice serves as the fundamental bedrock of political participation and the functional vitality of democratic systems. In this context, emigration represents the most extreme manifestation of exit [7].

Hirschman's seminal work predominantly explores the implications of emigration within the purview of small states, while largely overlooking the political and security ramifications of an alternative manifestation of exit, known as internal exit. Internal exit ensues when individuals, whether willingly or involuntarily, become detached from the political, economic, cultural, and social fabric of the country in which they reside. This isolation predominantly emanates from an amalgamation of factors, with political and economic alienation assuming paramount significance. The extent of loyalty towards a country's macrostructures exhibits an inverse correlation with the prevalence of internal exit within the populace. Consequently, the level of loyalty also correlates with the potency of foreign narratives that promulgate the strategic interests of alternative nations.

There are clear signs revealing a conspicuous divergence between society and the government/state apparatus in Latvia and Lithuania, albeit to a somewhat lesser degree in Estonia. This divergence finds tangible expression in the markedly low levels of trust that society confers upon governmental institutions, thus engendering fertile terrain for nefarious actors to engage in influence operations and, by extension, realize their strategic objectives. From a defence standpoint, non-kinetic and hybrid operations could potentially garner support from the local population for the strategic objectives of the aggressor, provided that these objectives are adeptly formulated.

Given the comprehensive nature of contemporary warfare, which enmeshes an entire nation, defence endeavors must transcend traditional military domains. They must encompass the broader fabric of society, information systems, culture, politics, economics, and infrastructure, thereby engendering enhanced national resilience. Consequently, security and defence considerations necessitate an approach predicated on the notion of resilience. A resilient society epitomizes the capacity of individuals, collectively or individually, to react and rebound from crises. In a non-resilient society, some individuals may languish in a state of protracted convalescence, with prospects for full recovery remaining elusive [8]. The level of resilience exhibited by a society constitutes both a symptomatic indicator and a causative factor of a broad range of social and individual attitudes and values. These encompass external threats and interference, historical experiences, nationalistic pride, trust in armed forces and institutions, religious inclinations, conscription policies, alongside individual-level factors such as age, education, financial standing, marital status, place of residence, religious beliefs, and ideological convictions (Figure 6-1).



**Figure 6-1: Trust in Political Institutions in the Baltic Region. Own calculations based on the Eurobarometer 95.3, June – July 2021. EE = Estonia, LT = Lithuania, LV = Latvia.**

Within the Baltic Countries, Russia has strategically capitalized on local agents of influence, including non-governmental organizations, informal groups, journalists, academics, artists, opinion leaders, and even government officials, some of whom may be unwitting participants in these machinations. While the Baltic States' governments have diligently monitored the progress of these influence operations, their countermeasures have primarily relied on presenting the populace with factual information and critical analysis, as well as providing explicit and unequivocal communication regarding the nature of these operations, elucidating the identities of the assailants (if ascertainable), elucidating the objectives, expounding upon the propagated narrative, and debunking the fallacies therein. Prior to Russia's escalation in February 2022, Lithuania aside, there existed no prohibition on the dissemination of Russian television and radio broadcasts, except in cases involving hate speech and incitement to violence. However, in the wake of the escalation, the three Baltic Countries have enacted measures to prohibit numerous Russian television channels.

The non-military threats to the security of the Baltic Countries emanate from their inherent frailties and, in certain instances, the incongruity between security and strategic aims and political and economic interests. Following their attainment of independence, the primary political aspiration of these nations revolved around integration with the Western sphere and its central institutions, such as the European Union, the Organisation for Economic Co-operation and Development (OECD), and NATO, thereby extricating themselves from the sphere of Russian influence. Nonetheless, the post-independence economic policies, particularly in Latvia, placed significant emphasis on positioning themselves as conduits for bridging the realms of finance and logistics/transit between the East and the West, inevitably entailing Russia assuming a prominent role as their principal partner.

Given the intricate interdependence of economics and politics, it was inevitable that Russia would assert a modicum of indirect influence. While endeavors to divert the trajectory of political and economic integration with the West have proven futile, Russia has adroitly exploited economic interests as a means of amassing political leverage and influence. Subsequent to the annexation of Crimea, the focus has shifted towards fomenting populist sentiments, particularly those that antagonize the West, neoliberal globalization, homosexuality, pseudo-traditional values, scientific skepticism, vaccine hesitancy, and similar ideological currents.

### **6.3 POLITICAL**

Russia's endeavors to influence Latvian politics can be categorized into three distinct levels. Firstly, Russia employs a strategy of supporting pro-Russian political parties, organizations, non-governmental organizations, and individuals. Secondly, it aims to maintain or increase its political influence over the local population. Lastly, Russia seeks to exert its influence by targeting politicians and civil servants, primarily at the regional level.

The primary pro-Russian political force in Latvia was the political alliance known as Harmony. Initially established as Harmony Center in 2005 through the merger of the National Harmony Party, the Socialist Party of Latvia, the New Center, the Daugavpils City Party, and the Social Democratic Party, the coalition underwent a consolidation process in 2010 and 2011, eventually evolving into the Social Democratic Party Harmony. Notably, in 2009, the party signed a cooperation agreement with United Russia, the party associated with President Putin, as well as A Just Russia, considered a sub-party under United Russia. Additionally, in 2011, the party signed a cooperation memorandum with the Chinese Communist Party, followed by its membership in the European Socialist Party in 2015. It is worth mentioning that in 2017, the party distanced itself from United Russia in an attempt to enhance its appeal within Latvian mainstream politics and secure inclusion in the government's coalition. Nils Ušakovs, a prominent figure within Harmony, held the mayoral position in Riga for a decade, spanning from 2009 to 2019.

While asserting that Russia exercises direct control over any specific political party in Latvia is difficult, numerous politicians maintain close contact with Russian political actors. In a 2015 interview with the Russian radio station Ekho Moskvi, former Russian Ambassador to Latvia Viktor Kalyuzhny revealed that the Russian Embassy had devised a plan for a pro-Russian coalition to govern Riga's city council by 2009 and secure the majority of seats in the Parliament during the 2010 elections.<sup>2</sup> Kalyuzhny expressed regret that while the plan succeeded with regard to the Riga City Council, it did not achieve the same outcome in the Parliament due to the different objectives of his successor. He also mentioned advising Harmony's leader Jānis Urbanovičs to make way for new faces, possibly alluding to Nils Ušakovs. Both politicians denied their involvement in any plan orchestrated by the Russian Embassy.<sup>3</sup> Since 2017, Harmony has publicly distanced itself from Russia and adopted a social democratic profile to compete with predominantly conservative ethnic Latvian parties. The party has maintained a stable electorate, securing an average of 25% of the seats in Parliament, but has never participated in the government coalition.

Russia's actions also seek to convince the local population that they face discrimination and to undermine the legitimacy of the political and economic model, including Latvia's alignment with Western values. Following Latvia's independence from the Soviet Union in 1991, automatic citizenship restoration was granted to all individuals who were citizens prior to 1940, along with their descendants, irrespective of their ethnic background. Conversely, those who migrated to Latvia from the Soviet Union between 1940 and 1991 had to apply for citizenship.<sup>4</sup>

This policy created discontent among some individuals, who felt insulted by the distinction. Russia has capitalized on this discontent as part of its Russkiy Mir policy, ostensibly supporting and protecting Russian speakers. In practice, Russia has endorsed initiatives aimed at impeding the full integration of Russian-speaking Latvians into the country. However, it is erroneous to perceive the Russian-speaking population in Latvia and the Baltic States as a fifth column predisposed to supporting Russian destabilization efforts in the region. The identity of the Russian-speaking population is diverse, and the majority are not necessarily pro-Russian.

Education represents a sensitive issue in this context. Following independence from the USSR, Latvia maintained the Soviet dual-language education system, offering instruction in both Latvian and Russian languages. Each language had its own educational program and materials, resulting in significant disparities in learning outcomes, particularly in subjects such as History. In 2002, the Latvian government initiated a program aimed at safeguarding the cultural heritage of minorities residing in Latvia, leading to the establishment of publicly funded schools offering education in seven different languages.<sup>5</sup>

Beginning with the 2019/2020 school year, new regulations governing minority education were implemented. Prior to this, 60% of studies were to be conducted in Latvian, with the remaining 40% in the minority language. Over a transitional period between 2019/2020 and 2021/2022, a gradual shift towards instruction solely in Latvian was mandated, with exceptions made for language and literature, as well as disciplines related to the culture and historical aspects of the respective minority group. Harmony Center, the political party, attempted to block this initiative in Parliament and subsequently appealed to the President to prevent the law from being enacted. Protests organized by pro-Russian politicians, such as Tatjana Ždanoka, failed to exert any political impact.<sup>6</sup> The reform is progressing as planned.

---

<sup>2</sup> See <https://echo.msk.ru/sounds/1506612.html>, in Russian.

<sup>3</sup> See <https://skaties.lv/zinas/latvija/politika/urbanovics-un-usakovs-noliedz-krievijas-programmas-istenosanu-latvija/>, in Latvian.

<sup>4</sup> To receive full citizenship, each applicant must pass tests to demonstrate Latvian language skills, the lyrics of their national anthem, and basic knowledge of Latvian History; they are also required to swear loyalty to the Latvian state. The status of non-citizen entitles the same rights of a citizen with the exception of voting and working in the public sector.

<sup>5</sup> Russian, Polish, Hebrew, Ukraine, Estonian, Lithuanian, and Belorussian.

<sup>6</sup> See <https://www.lsm.lv/raksts/zinas/latvija/protesta-pret-macibam-tikai-latviski-pulcejas-1500-cilveki-bez-starpgadijumiem.a317696/>

Russia has also sought to exploit local pseudo-activists and “governmental-non-governmental” organizations funded by the Kremlin to destabilize Latvia. Although the financial resources allocated to these entities are relatively modest, they fuel the Kremlin’s paranoia about the West, fabricating or magnifying issues disconnected from reality to ensure continued funding. It is reasonable to conclude that these entities have the least interest in protecting minorities, as resolving the purported issues they claim to champion would render them irrelevant and leave the pseudo-activists unemployed. These entities have championed five initiatives over the past decade aimed at destabilizing Latvia, including the aforementioned education in Russian, establishing Russian as Latvia’s second official language, automatic citizenship for all non-citizens, granting autonomy to the region of Latgale, and promoting a morals and family initiative.

The initiative advocating for Russian to become Latvia’s second official language has a dual purpose. Firstly, it aims to counter the process of derussification that Latvia has undergone since its independence, at least to some extent. By making Russian an official language, the educational reform discussed earlier would be averted. Secondly, it aligns with a broader strategy aimed at establishing Russian as one of the official languages of the European Union.<sup>7</sup> On March 4, 2011, the youth movement “United Latvia” collaborated with the Association “Native Language” to collect signatures for proposing amendments to the Latvian constitution, permitting Russian to become the country’s second official language.<sup>8</sup> The political party “For Human Rights in a United Latvia” (since 2014 known as “Latvian Russian Union”) soon declared its support for this initiative.<sup>9</sup>

The petition, containing 12,533 signatures, was submitted to the Central Election Commission in September 2011. From November 1 to 30, 2011, an official signature collection took place, resulting in the collection of 187,378 signatures, surpassing the required 154,379. The proposal was subsequently submitted to the President, who forwarded it to the Parliament for consideration. As the amendments were ultimately rejected, a national referendum was deemed necessary. The referendum took place on February 18, 2012.<sup>10</sup>

Certain political parties attempted to obstruct the initiative by initiating a discussion about its legality. However, the Supreme Court concluded that the initiative was constitutional. The referendum garnered participation from 1,098,593 citizens with voting rights, accounting for 70.73% of the electoral college. Of these participants, 821,722 (74.8%) voted against the amendments, while 273,347 (24.88%) voted in favor. The Russian Ministry of Foreign Affairs protested the results, contending that non-citizens were not allowed to vote, thus claiming that the outcome did not reflect reality. Nevertheless, even if all non-citizens, regardless of age (312,189 in 2012), were permitted to vote, the result would remain unchanged, albeit with a different proportion between “against” and “for.”<sup>11</sup>

On September 4, 2012, the political party “For Human Rights in a United Latvia” submitted a petition to the Central Election Commission, consisting of 12,686 signatures. The petition called for the granting of Latvian citizenship to all non-citizens as of January 1, 2014, unless they submitted an application to retain their non-citizen status. Although the number of signatures was sufficient to initiate an official signature collection, the Central Election Commission expressed doubts about the constitutional validity of the proposed amendment. Various institutions, including the Chancellery of the President, the Legal Bureau of the Saeima

---

<sup>7</sup> A language may attain official status in the European Union if one of its member states recognizes it as one of its official languages.

<sup>8</sup> Until 2012 the Latvian law permitted that at least 10,000 citizens of Latvia with voting rights have the right to lodge a fully drawn-up draft law or draft amendments to the Constitution to the Central Election Commission, which will organize a referendum. The current redaction changed the number to ten percent of the citizens with voting rights.

<sup>9</sup> See <https://web.archive.org/web/20150220171222/http://vienotalatvija.lv/index.php?limitstart=35&lang=lv> and [https://web.archive.org/web/20140815043533/http://zapchel.lv/?lang=ru&mode=archive&submode=year2011&page\\_id=11033](https://web.archive.org/web/20140815043533/http://zapchel.lv/?lang=ru&mode=archive&submode=year2011&page_id=11033)

<sup>10</sup> See <https://www.cvk.lv/parakstu-vaksanas/parakstu-vaksanas-lidz-2012-gadam/parakstuvaksana-par-grozijumu-satversme-ierosinasanu-2011-gada-novembris>, in Latvian.

<sup>11</sup> In this case, it would have been 58.4% against and 41.4% for (own calculations based on data from the Central Election Commission and the Central Statistics Office of Latvia).

(Latvian Parliament), the Ministry of Justice, the Ministry of the Interior, the Ministry of Foreign Affairs, and several law faculties, were consulted to provide opinions on the matter. The initiative's proponents were also given an opportunity to express their views. On November 1, 2012, the Central Election Commission determined that the initiative should not proceed to the signature collection stage.<sup>12</sup>

While the Central Election Commission deliberated on the legality of the citizenship initiative, the leader of the party "Native Language," Vladimirs Lindermanis, began advocating for the establishment of an autonomous Latgale region. In an interview with the Latvian news agency LETA, published on October 9, 2012, Lindermanis stated that "it is evident that the authorities are doing everything to delay and prevent the citizenship referendum. There must be an appropriate response, and I believe that Latgale's autonomy within Latvia is such a response."<sup>13</sup>

On December 5, 2012, a search was conducted by the Security Police at Lindermanis' residence, resulting in the confiscation of a computer, CDs, and flash drives. Similar searches and seizures of hardware took place at the homes of other activists. Three days later, Lindermanis traveled to the city of Daugavpils to lead a conference on Latgale's autonomy. However, the event attracted only a few attendees. The leaders of Harmony Center, Jānis Urbanovičs and Nils Ušakovs, dismissed the idea as unproductive and a hallucination, respectively. Lacking support, the initiative fizzled out on its own.

Arguably, the most successful initiative to influence Latvian politics thus far has been the Tikumība (Morals) initiative. Notably, this case brought together pro-Russian political agents and Latvian nationalists in a shared endeavor to promote family values based on myths propagated by Russian agents of influence. One prevalent falsehood was the myth of infant rape and incest as a social tradition in Norway. This myth was disseminated through two channels. Firstly, a celebrity anesthesiologist named Pēteris Kļava claimed in an interview that "in Norway, there are special classes for children teaching them how to recognize when their fathers have crossed the line" and that "this was a suggestion made by a Norwegian minister, who stated in an interview with a Russian publication that incest in Norway is a social tradition." Secondly, during a conference on gender equality and policy financed by Norway, the dean of the University of Latvia's Stradins Faculty of Law asserted that Norway is a pedophiles' paradise and that the European Union is advocating for the legalization of pedophilia.<sup>14</sup> Secondly, during a conference on gender equality and policy financed by Norway, the dean of the University of Latvia's Stradins Faculty of Law asserted that Norway is a pedophiles' paradise and that the European Union is advocating for the legalization of pedophilia.<sup>15</sup>

In 2013, the NGO "Let's Save our Children" began collecting signatures for a referendum aimed at banning the promotion of sex education. This initiative coincided with Russia's enactment of legislation imposing fines for the promotion of homosexuality among minors. One year earlier, Russia had also passed two laws aimed at combatting the dissemination of information that goes against family values and blocking internet pages without a court decision. However, the plans for the referendum did not succeed, as Christian Latvians involved in the organization refused to accept Vladimirs Lindermanis as its main leader.

The initiative gained political traction after former Harmony member of Parliament Irina Cvetkova witnessed a protest organized by the NGO Dzintars (Family). Following her meeting with the organization's leadership, she proposed an amendment to the Law for Children Protection that would prohibit the promotion of sex education in schools. However, she failed to garner support from her own party. Cvetkova

---

<sup>12</sup> See <https://www.cvk.lv/lv/parakstu-vaksanas/parakstu-vaksanas-lidz-2012-gadam/parlikumprojekta-grozijumi-pilsonibas-likuma-ierosinasanu-2012>, in Latvian.

<sup>13</sup> Author's translation from "Redzam, ka valdošie grib aizliegt pilsonības referendumu, dara visu, lai novilcinātu laiku un beigās to vispār aizliegtu. Uz šādu rīcību jābūt kādai adekvātai atbildei un domāju, ka Latgales autonomija Latvijas sastāvā būtu šāda atbilde." See <https://nra.lv/latvija/81267-drosibas-policija-verte-lindermana-izteikumus-par-latgales-autonomijas-ideju.htm>

<sup>14</sup> See <http://www.mklat.lv/mnenie/24547-peteris-klyava-demokratiya-s-zapakhom-pedofilii>

<sup>15</sup> See <https://www.diena.lv/raksts/latvija/zinas/rsu-profesoram-parmet-norvegijas-nomelnosanu14178021>

subsequently left the party along with another member and, along with five colleagues from Zatlērs' Reform Party, presented the amendment for consideration. To support the importance of the amendment, Cvetkova made claims that incest is considered normal in Norway and is a social tradition. These allegations were substantiated by the documentary "TransNorway," which depicted non-gendered kindergartens in Sweden, a Norwegian millionaire donating the equivalent of €3.2 million to promote homosexuality in schools, and families allowing children to choose their own gender. However, these allegations are unfounded.

In 2015, the Latvian Parliament approved an amendment to the Law of Education, stipulating the removal of all immoral material from educational books. This amendment received significant support from Latvian nationalist parties. Additionally, amendments were made to the constitution, including a definition of what constitutes a Latvian family, namely a heterosexual couple with children. In recent years, Russian agents of influence have shifted their focus from citizenship and minority issues to concerns regarding immorality and the perceived decadence of the West. Considering the disruptive nature of globalization, which has been eroding traditional ways of life, this field of discourse can be considered fertile ground for their endeavors.

In the most recent parliamentary election in 2022, two populist political parties secured 18 seats in the Saeima (Parliament). Although it is not possible to establish a direct connection between these parties and the Kremlin, their political agenda aligns with Russian narratives, worldview, foreign policy objectives, and economic policies, including a rejection of the West. These parties have consistently and vigorously demanded the dissolution of the current government and new elections, and their popularity has been on the rise, with one of them ranking as the third most popular party in recent polls.

## **6.4 ECONOMIC AND SOCIAL**

The examination of the economic platforms of political parties elected to the 5th – 8th Saeima (the Latvian Parliament) reveals a prioritization of transit, real estate, and finance as key sectors for development [9]. These sectors have exhibited significant dependence on financial inflows from Russia and the Commonwealth of Independent States (CIS), thereby establishing business interests as a substantial conduit for Russian influence. The presence of dubious origins of certain assets within these sectors has also raised concerns regarding money laundering and corruption, consequently tarnishing Latvia's reputation.

In essence, the emphasis on finance, real estate, and transit has contributed to the deindustrialization of Latvia and the contraction of the services sector, resulting from a lack of competitiveness stemming from an overvalued exchange rate. This has led to an economic reorganization that favors speculative and/or non-sustainable sectors, such as the consumption of durable goods [10]. In other words, the country's competitiveness has relied on low wages rather than the establishment of a multifaceted economy driven by high-productivity sectors capable of exporting high-value-added goods. Although Latvia's economy has demonstrated growth and development, it remains insufficient in comparison to other countries, perpetuating a continuous state of inadequate development.

Nonetheless, Russia's capacity to exert economic influence on Latvia is highly limited. The majority of Latvia's external trade is conducted with European Union (EU) and NATO member states. In 2019, 72% of Latvia's exports were directed to EU member states, while 11% were destined for non-EU NATO member states. Conversely, exports to Russia accounted for only 9% of the total. Similarly, Latvia's imports from EU member states constituted 75% of the overall imports, with 8% originating from non-EU NATO member states and 7% from Russia. The transit sector, which has predominantly relied on Russia, represents 8% of Latvia's GDP, while the national air carrier Air Baltic is responsible for 3%.

Latvia has faced long-standing allegations of money laundering involving funds from Russia and the former Soviet Union. However, since 2017, the country has faced pressure from the United States to tighten its anti-money laundering legislation. American officials were surprised to discover that five banks operating in

Latvia were circumventing international sanctions against North Korea, and the imposed fines were deemed insignificant, with the leading local bank, ABLV, evading punishment. ABLV was accused of engaging in “institutionalized money laundering,” and an investigation into the suspected bribery of the Bank of Latvia’s governor was initiated. In mid-2019, the Latvian Saeima enacted an anti-money laundering law in an effort to avoid being placed on the gray list by Moneyval.

Among the Latvian population, a popular narrative emerges that encompasses the sentiment of “I love this land, but I hate this country.” While Latvia’s transition to a market economy can be considered successful, one of the foundational pillars of its economic policy has been the promotion of low wages as a means to establish competitiveness. Consequently, this has led to the development of a low-complexity economy characterized by low productivity and the production of goods with limited added value. As a result, economic growth has not translated into improved relative living standards. On the contrary, it has exacerbated wealth inequality and heightened sentiments of relative deprivation among the population.<sup>16</sup> The global financial crisis of 2008 further aggravated this situation, causing a decline in absolute living standards and prompting a significant portion of the population to emigrate or harbor resentment towards the State and the political system. Therefore, due to its limited economic leverage, Russia has focused on discrediting the Western neoliberal financial system and Latvia’s economic model. However, Latvia has implemented policies to address these issues, including the increase of wages and the development of sectors with higher economic complexity, such as Information Technology (IT).

## **6.5 DIPLOMATIC AND INFORMATIONAL**

Russia’s diplomatic and information actions in Latvia aim to undermine its credibility, particularly within NATO, the European Union, and the United States. Russia focuses on five specific issues in its diplomatic efforts against Latvia. Firstly, it promotes the idea that the Baltic States were liberated from fascism by the Red Army and voluntarily joined the USSR, rather than being forcibly annexed. This is exemplified by recent tweets from the Russian Embassy in Latvia, which present a Russian interpretation of Latvia’s occupation and annexation by the Soviet Union. This narrative suggests that Latvia willingly joined the Soviet Union and denies the notion of annexation and occupation. It is part of Russia’s broader efforts to portray the Soviet Union as a victim and justify the Molotov-Ribbentrop Pact as a means of self-preservation and maintaining peace.

Since 2002, there has been an ongoing process of “passportization” by Russia in Latvia, targeting two main groups:<sup>17</sup> non-citizens and individuals willing to receive Russian pensions.<sup>18</sup> This increase in Russian citizens provides Russia with a stronger pretext for intervention in Latvia, considering the notion of protecting compatriots abroad, which was previously used as an excuse for Russian military interventions in Georgia and Ukraine. However, for many individuals, acquiring Russian citizenship is primarily an economic decision to receive a pension earlier and supplement regular income in Latvia, rather than an automatic expression of allegiance and loyalty to Russia.

Thirdly, Russian diplomats seek to establish contact with regional governments with the aim of renovating Soviet military memorials. Simultaneously, the Russian Embassy actively identifies and recruits potential individuals and organizations involved in research and conservation work related to Russian history, culture clubs, and military archaeology groups. Russian information operations in Latvia are designed to shape public opinion by promoting specific interpretations of certain issues within particular social groups.

---

<sup>16</sup> Relative deprivation refers to the subjective judgment that one is worse off or deprived of some state or thing in comparison to some standard [11].

<sup>17</sup> In 2002, the acquisition of Russian citizenship was simplified for any citizen of the former Soviet Union, irrespective of the current country of residence.

<sup>18</sup> Until 2018, Russia kept the Soviet Union retirement age of 55 years for women and 60 years for men. In Latvia it is currently 63 years and six months to reach 65 by 2025.



The ultimate objective is to generate and reinforce discontent with the current political, cultural, and economic model in Latvia and to foster rejection of Western values [12].

The main instruments employed are disinformation articles in Russian and Latvian media, as well as the use of social media “trolls” to spread fake news or share opinions that often revolve around discrimination in Latvia, the alleged moral decay of Western society, and agreement with Russian narratives. Russia employs several key narratives [12]:

- 1) Russian-speaking minorities are marginalized and treated unfairly by the government.
- 2) The Baltic States are failed states and corruption is widespread.
- 3) EU membership resulted in economic and social underdevelopment. Latvia should follow its own path without foreign interference.
- 4) EU membership is tantamount to being a USSR republic.
- 5) NATO membership decreases the overall level of security because of possible Russian countermeasures.
- 6) Western values are corrupted. Tolerance towards homosexuals and other minorities is presented as the moral degradation of traditional family's values.
- 7) There is no real democracy in the West. Politicians are puppets controlled by the financial system and work against the real interests of the population.
- 8) Fascism is glorified in the Baltics.

The anti-Western narrative primarily seeks to highlight the alleged decadence of the West, covering issues ranging from economic and social problems to the acceptance of homosexuality and pedophilia. Although the governments of the Baltic States closely monitor these influence operations, counteraction involves presenting the population with facts and critical information and directly addressing such operations in clear language. This includes identifying the attackers (if known), outlining their objectives, explaining the narrative being propagated, and providing reasons why it is untrue [12]. Prior to the escalation of Russia's war against Ukraine, there were no restrictions on the broadcasting of Russian television and radio, unless cases involved hate speech or incitement to violence. However, since February 2022, the media regulators of the Baltic states have prohibited the retransmission of many Russian-language channels deemed to spread Russian disinformation.

## **6.6 ENERGY**

An important question pertains to Latvia's energy security, which holds particular significance due to historical ties with Russia that were deepened during the Soviet period. The first issue revolves around Latvia's reliance on gas imports from Russia. The second issue concerns the Baltic States' interconnection with Russia's power grid. The third issue involves the import of electricity from Russia. These factors expose Latvia to strategic vulnerabilities, as Russia allegedly has the ability to disrupt the electricity system in the Baltics or cut off gas supplies during winter. However, the reality is more nuanced.

Latvia possesses an underground gas storage facility in Inčukalns with a capacity of 4.47 billion cubic meters. Of this, 2.3 billion cubic meters are actively utilized, equivalent to approximately two years of Latvia's natural gas consumption. It is possible to increase the active reserves to 3.2 billion cubic meters. The country has been engaged in collaborative efforts with Estonia and Lithuania to explore alternative energy sources, aiming to reduce and eventually eliminate reliance on Russian gas.

Despite three decades having passed since their separation from the Soviet Union, the Baltic States remain synchronized with Russia's power grid to ensure stable power supply and prevent blackouts. Some analysts

argue that in the event of a conflict, Russia could disconnect the electricity supply to the Baltic States. While technically feasible, such an action would also result in power outages in Kaliningrad, Russia's western region, including Saint Petersburg, and a significant portion of Belarus. In response, the Baltic States have plans to fully disconnect from the Russian power grid and connect to the European power grid by 2025. In anticipation, Russia has initiated the construction of a power plant in Kaliningrad to ensure self-sufficiency for the region. There are purported plans to disconnect the Baltic States from the Russian power grid as early as 2024.

Regarding Latvia's dependence on imported electricity, the country produced 6,178 million kilowatt-hours in 2019, while consumption reached 7,296 million kilowatt-hours. In 2018, energy production amounted to 6.5 million kilowatt-hours. In other words, Latvia is nearly self-sufficient in terms of electricity production.

## **6.7 FINAL REMARKS**

Non-kinetic instruments of warfare have garnered increasing significance in the pursuit of military strategic objectives, blurring the conventional demarcation between military and non-military means of warfare. Concurrently, kinetic instruments may be employed to achieve non-military strategic goals, thereby complicating the traditional categorization of military and non-military methods of warfare. Consequently, the initial step in assessing the instruments a nation might employ against an adversary is to ascertain its strategic objectives.

In the realm of open-source discussions, Russia's strategic aim in the Baltic States is often described as "finlandization," a process that can be realized through either kinetic or non-kinetic means, or a combination thereof. Thus far, Russia has primarily relied on non-kinetic methods in its dealings with the Baltic States. This approach can be attributed to the presence of NATO's reassurance and deterrence measures, as well as the Baltic States' fortification of their defence capabilities. Therefore, the salience of military deterrence in the region should not be underestimated. It is important to note that the operationalization of non-kinetic warfare, particularly information, psychological, and influence operations, heavily relies on exploiting the specific vulnerabilities of the opponent. As a result, deterrence primarily assumes the form of denial, surpassing the purview of the military and entering the realm of politics.

Russian influence operations in Latvia have adhered to the methodologies and tenets expounded in Russian military literature. Nevertheless, their efficacy has been limited. Russia has been unable to capitalize on economic interests due to Latvia's alignment with Western economies. The prioritization of European Union (EU) and NATO membership, along with recent OECD accession, as crucial objectives of Latvian foreign policy, has compelled internal political actors to recalibrate their interests accordingly, thereby diminishing Russia's economic and political leverage.

Political operations undertaken by Russian agents of influence have predominantly yielded meager results, save for the moral initiative. Diplomatic and information operations have also been constrained, resulting in circumscribed impact. The Latvian populace harbors a natural suspicion regarding Russia's intentions, while Russia has failed to project itself as an alluring and viable alternative to the West. Consequently, Russia has shifted its strategy from pro-Russian objectives to anti-Western objectives. Given the idiosyncrasies of the Neoliberal Western model of political and economic governance, ample opportunities exist for Russia to exploit vulnerabilities in influence operations. It is incumbent upon the political elite to engage in sincere self-criticism, identifying and addressing these vulnerabilities in order to diminish Russia's leverage and mitigate the influence of other potential malign actors.

## 6.8 REFERENCES

- [1] Bērziņš, J. “The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria.” *The Journal of Slavic Military Studies*, 33(3), 2020, pp. 355-380. <https://doi.org/10.1080/13518046.2020.1824109>
- [2] Kremlin. Podpisan zakon o popravke k konstitutsii rossiyskoy federatsii. [The law on amendments to the constitution of the russian federation.] 2020. <http://kremlin.ru/acts/news/62988>
- [3] Simindey, V. Etnopoliticheskaya model' postsovetskoy Latvii: Tendentsii i razvitiye. [“The Ethnopolitical Model of Post-Soviet Latvia: Trends and Development.”] *Mezhdunarodnaya zhizn*, 3, 2019, pp. 139-145.
- [4] Skachkov, A. Rossiya i Pribaltika: Prichiny krizisa. [“Russia and the Baltics: The Causes of Crisis.”] *Mezhdunarodnaya zhizn*, 9, 2018.
- [5] Voronov, K. (2019). Strategii mezhdunarodnoy adaptatsii malykh stran: Satellizm vs. finlyandizatsiya. [“Strategies for the International Adaptation of Small Countries: Satellitism vs. Finlandization.”] *Mezhdunarodnaya zhizn*, 5, 2018.
- [6] Nagorny, A., and Shurygin, V. (eds.). “Defense Reform as an Integral Part of a Security Conception for the Russian Federation: A Systemic and Dynamic Evaluation.” *Izborsky Club*, 2013.
- [7] Hirschmann, A. “Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States.” *Harvard University Press*, 1970.
- [8] Brunnermeier, M.K. *The Resilient Society*. Endeavor Literary Press, Colorado Springs, CO, 2021.
- [9] Bērziņš, J. *Macroeconomic Policy, Business Cycles, and Neoliberalism in Latvia* (PhD Thesis). University of Latvia, 2015.
- [10] Bērziņš, J. “Ignacio Rangel Visits Latvia: Crisis and the Political Economy of Duality.” *Debate: Journal of Contemporary Central and Eastern Europe*, 22(1), 2014, pp. 81-102. <https://doi.org/10.1080/0965156X.2013.873190>
- [11] Williams, R. M. “Relative Deprivation.” In L.A. Coser (ed.), *The Idea of Social Structure: Papers in Honor of Robert K. Merton*. Routledge, 2017, pp. 355-378.
- [12] Bērziņš, J. “Integrating Resilience in Defense Planning Against Information Warfare in the Post-Truth World.” In V. Norman, B. Ang, and S. Jayakumar (eds.), *Drums: Distortions, Rumours, Untruths, Misinformation, and Smears*, World Scientific, 2018, pp. 117-131.



## Chapter 7 – CONCLUSION

The case studies presented in this volume highlight a number of important planning considerations for the Alliance and its partners. First, national level legal frameworks must be relevant to contemporary and expected future conditions of the operational environment. This is foundational as it sets the conditions for Alliance members and partners to contribute relevant and credible national capabilities to collective security and defence. Second, Russia will tailor its behaviors to the context of individual national targets. As both Bērziņš and Reader show, this might lead to targeting paths that are incongruent with national planning assumptions. Third, collectively, the case studies suggest that a major conclusion of the SAS-121 analysis – that Ukraine’s national context presented unique opportunities for Russian exploitation – remains valid. While some socio-cultural factors are shared with other Eastern European nations (e.g., ethnic Russian communities or Russian-speaking enclaves), each must be considered within individual national contexts. Fourth, Alliance support to partners must be coordinated and deconflicted and include, as much as possible, non-Alliance countries that are also seeking to contribute to partner nation capability and capacity development. Finally, the case studies reinforce that collective security and defence is only as strong as the national level arrangements that form the foundations of deterrence. Gaps at the national level, for both Alliance and like-minded partners, will undermine the whole. In this regard, national conceptions of total or comprehensive defence, aligned with relevant legal and policy frameworks, are critical. Holistic national approaches to security and defence are the foundation for effective counters to expected Russian behavior.

## CONCLUSION

---



## Annex A – TABLE OF IMPLICATIONS – SOURCE MATERIAL

This table indicates the relationship between the various components of RTG research and analysis and the individual military implications detailed in Volume V.

Military Implication Title	Source Material
Developing Common Understanding	CAN, DNK (KFOR), GBR
Systematic Analysis of Military Exercises	GBR, SWE
Spirituality and Religion	DNK (KFOR)
Religious Organisations and Politics	DNK (KFOR)
National Interests, Alliances, and Partners	UKR
Reducing Coercive Options: Limiting Dependence	UKR
Formulating Legal Frameworks	CZE, HRV, UKR, NSHQ
NATO Capability and Capacity Building	NSHQ
NATO-UN Partnerships	DNK (KFOR)
Article 5, Hybrid Methods, and Alliance Cohesion	GBR, NSHQ
Indications, Warnings, and Article 4	GBR
Finding Common Ground	DNK (KFOR)
Adapting Force Structure	UKR, NSHQ
Situational Picture and Awareness	CZE, FIN, HRV, UKR
Wartime Military Effectiveness	UKR
NATO Operational Planning: Long-Term Threat	All material
Laws of War	UKR, NSHQ
Integration of Military and Non-Military Capabilities	UKR, NSHQ
Ukraine’s Information Security: Mental Resilience	UKR
Strategic Communications and Internal Resilience	UKR
CIMIC in a National/Allied Context	DNK (KFOR)
Exercise Analysis: Frontstage (Public), Backstage (Veiled) and Mystification	CAN, SWE
Military Strategies to Handle Russian Backstage and Frontstage Acting	SWE
The Application of the Military Instrument of Power (MIOP)	GBR
MIOP Backstopping Hybrid Activity	GBR, SWE, UKR
Electronic Warfare: Prevention and Protection	FIN, HRV, SWE
Homeland Defence is the Bedrock of Alliance Cohesion	CZE, FIN, HRV, UKR
National Homeland Defence Concepts	CZE, FIN, GBR, HRV, NSHQ

**ANNEX A – TABLE OF IMPLICATIONS-SOURCE MATERIAL**

<b>Military Implication Title</b>	<b>Source Material</b>
Business and Investment – The Economic Instrument of Power	FIN, HRV
Influence on Non-Governmental Organizations	DNK (KFOR), FIN, HRV
Homeland Defence: Readiness	All material
Strategic Communication in Transition: ‘Total War’ to ‘Post-(Major) Conflict’	UKR
NATO Strategic Communications and Shared Understandings	All material
Countering Russian Rhetoric	All material
Focus on the Effect	CAN, GBR, UKR
Minor Actions Matter	CAN, GBR, UKR
Operational Security	CAN, FIN, GBR, UKR



<b>REPORT DOCUMENTATION PAGE</b>			
<b>1. Recipient's Reference</b>	<b>2. Originator's References</b>	<b>3. Further Reference</b>	<b>4. Security Classification of Document</b>
	STO-TR-SAS-161-VOL-III AC/323(SAS-161)TP/1174	ISBN 978-92-837-2486-5	PUBLIC RELEASE
<b>5. Originator</b>	Science and Technology Organization North Atlantic Treaty Organization BP 25, F-92201 Neuilly-sur-Seine Cedex, France		
<b>6. Title</b>	The NATO STO SAS-161 Research Task Group (RTG) – Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices Volume III: Comprehensive Defence, Capacity Building, and Enhanced Forward Presence		
<b>7. Presented at/Sponsored by</b>	This volume of SAS-161 presents case studies from Czechia, Great Britain, Latvia, Ukraine, and NSHQ, related to comprehensive defence, capability and capacity building, and enhanced forward presence.		
<b>8. Author(s)/Editor(s)</b>	Multiple		<b>9. Date</b> October 2023
<b>10. Author's/Editor's Address</b>	Multiple		<b>11. Pages</b> 100
<b>12. Distribution Statement</b>	There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.		
<b>13. Keywords/Descriptors</b>	Baltic states; Capacity building; Comprehensive defence; Enhanced forward presence; Finlandization; Hybrid; Influence activities; Information activities; NSHQ; Russia; Sabotage; SOF; Territorial defence forces; Total defence		
<b>14. Abstract</b>	The NATO STO SAS-161 Research Task Group (RTG) investigating “Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices” is meant to inform the full spectrum of military planning at the Alliance and national level. The functionally oriented analysis and the country-specific case studies developed by the RTG touch all aspects of military effectiveness and help inform our collective efforts to account for the challenges of contemporary, and expected future characteristics, of competition, conflict, warfare, and warfighting. This volume presents case studies detailing considerations for the design of comprehensive defence at the national level, the design of capability and capacity building activities in support of partner countries, and lessons related to national deployments in support of Alliance Enhanced Forward Presence activities.		





BP 25

F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE  
Télécopie 0(1)55.61.22.99 • E-mail [mailbox@cs.o.nato.int](mailto:mailbox@cs.o.nato.int)



**DIFFUSION DES PUBLICATIONS  
STO NON CLASSIFIEES**

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre et la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (<http://www.sto.nato.int/>) et vous abonner à ce service.

**CENTRES DE DIFFUSION NATIONAUX**

**ALLEMAGNE**

Streitkräfteamt / Abteilung III  
Fachinformationszentrum der Bundeswehr (FIZBw)  
Gorch-Fock-Straße 7, D-53229 Bonn

**BELGIQUE**

Royal High Institute for Defence – KHID/IRSD/RHID  
Management of Scientific & Technological Research  
for Defence, National STO Coordinator  
Royal Military Academy – Campus Renaissance  
Renaissancelaan 30, 1000 Bruxelles

**BULGARIE**

Ministry of Defence  
Defence Institute "Prof. Tsvetan Lazarov"  
"Tsvetan Lazarov" bul no.2  
1592 Sofia

**CANADA**

DGSIST 2  
Recherche et développement pour la défense Canada  
60 Moodie Drive (7N-1-F20)  
Ottawa, Ontario K1A 0K2

**DANEMARK**

Danish Acquisition and Logistics Organization  
(DALO)  
Lautrupbjerg 1-5  
2750 Ballerup

**ESPAGNE**

Área de Cooperación Internacional en I+D  
SDGPLATIN (DGAM)  
C/ Arturo Soria 289  
28033 Madrid

**ESTONIE**

Estonian National Defence College  
Centre for Applied Research  
Riia str 12  
Tartu 51013

**ETATS-UNIS**

Defense Technical Information Center  
8725 John J. Kingman Road  
Fort Belvoir, VA 22060-6218

**FRANCE**

O.N.E.R.A. (ISP)  
29, Avenue de la Division Leclerc  
BP 72  
92322 Châtillon Cedex

**GRECE (Correspondant)**

Defence Industry & Research General  
Directorate, Research Directorate  
Fakinos Base Camp, S.T.G. 1020  
Holargos, Athens

**HONGRIE**

Hungarian Ministry of Defence  
Development and Logistics Agency  
P.O.B. 25  
H-1885 Budapest

**ITALIE**

Ten Col Renato NARO  
Capo servizio Gestione della Conoscenza  
F. Baracca Military Airport "Comparto A"  
Via di Centocelle, 301  
00175, Rome

**LUXEMBOURG**

*Voir Belgique*

**NORVEGE**

Norwegian Defence Research  
Establishment  
Attn: Biblioteket  
P.O. Box 25  
NO-2007 Kjeller

**PAYS-BAS**

Royal Netherlands Military  
Academy Library  
P.O. Box 90.002  
4800 PA Breda

**POLOGNE**

Centralna Biblioteka Wojskowa  
ul. Ostrobramska 109  
04-041 Warszawa

**PORTUGAL**

Estado Maior da Força Aérea  
SDFA – Centro de Documentação  
Alfragide  
P-2720 Amadora

**REPUBLIQUE TCHEQUE**

Vojenský technický ústav s.p.  
CZ Distribution Information Centre  
Mladoboleslavská 944  
PO Box 18  
197 06 Praha 9

**ROUMANIE**

Romanian National Distribution  
Centre  
Armaments Department  
9-11, Drumul Taberei Street  
Sector 6  
061353 Bucharest

**ROYAUME-UNI**

Dstl Records Centre  
Rm G02, ISAT F, Building 5  
Dstl Porton Down  
Salisbury SP4 0JQ

**SLOVAQUIE**

Akadémia ozbrojených síl gen.  
M.R. Štefánika, Distribučné a  
informačné stredisko STO  
Demänová 393  
031 01 Liptovský Mikuláš 1

**SLOVENIE**

Ministry of Defence  
Central Registry for EU & NATO  
Vojkova 55  
1000 Ljubljana

**TURQUIE**

Milli Savunma Bakanlığı (MSB)  
ARGE ve Teknoloji Dairesi  
Başkanlığı  
06650 Bakanlıklar – Ankara

**AGENCES DE VENTE**

**The British Library Document  
Supply Centre**  
Boston Spa, Wetherby  
West Yorkshire LS23 7BQ  
ROYAUME-UNI

**Canada Institute for Scientific and  
Technical Information (CISTI)**  
National Research Council Acquisitions  
Montreal Road, Building M-55  
Ottawa, Ontario K1A 0S2  
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (<http://www.ntis.gov>).



BP 25

F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE  
Télécopie 0(1)55.61.22.99 • E-mail [mailbox@cs.o.nato.int](mailto:mailbox@cs.o.nato.int)



**DISTRIBUTION OF UNCLASSIFIED  
STO PUBLICATIONS**

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (<http://www.sto.nato.int/>) from where you can register for this service.

**NATIONAL DISTRIBUTION CENTRES**

**BELGIUM**

Royal High Institute for Defence –  
KHID/IRSD/RHID  
Management of Scientific & Technological  
Research for Defence, National STO  
Coordinator  
Royal Military Academy – Campus  
Renaissance  
Renaissancelaan 30  
1000 Brussels

**BULGARIA**

Ministry of Defence  
Defence Institute “Prof. Tsvetan Lazarov”  
“Tsvetan Lazarov” bul no.2  
1592 Sofia

**CANADA**

DSTKIM 2  
Defence Research and Development Canada  
60 Moodie Drive (7N-1-F20)  
Ottawa, Ontario K1A 0K2

**CZECH REPUBLIC**

Vojenský technický ústav s.p.  
CZ Distribution Information Centre  
Mladoboleslavská 944  
PO Box 18  
197 06 Praha 9

**DENMARK**

Danish Acquisition and Logistics Organization  
(DALO)  
Lautrupbjerg 1-5  
2750 Ballerup

**ESTONIA**

Estonian National Defence College  
Centre for Applied Research  
Riia str 12  
Tartu 51013

**FRANCE**

O.N.E.R.A. (ISP)  
29, Avenue de la Division Leclerc – BP 72  
92322 Châtillon Cedex

**GERMANY**

Streitkräfteamt / Abteilung III  
Fachinformationszentrum der  
Bundeswehr (FIZBw)  
Gorch-Fock-Straße 7  
D-53229 Bonn

**GREECE (Point of Contact)**

Defence Industry & Research General  
Directorate, Research Directorate  
Fakinos Base Camp, S.T.G. 1020  
Holargos, Athens

**HUNGARY**

Hungarian Ministry of Defence  
Development and Logistics Agency  
P.O.B. 25  
H-1885 Budapest

**ITALY**

Ten Col Renato NARO  
Capo servizio Gestione della Conoscenza  
F. Baracca Military Airport “Comparto A”  
Via di Centocelle, 301  
00175, Rome

**LUXEMBOURG**

See Belgium

**NETHERLANDS**

Royal Netherlands Military  
Academy Library  
P.O. Box 90.002  
4800 PA Breda

**NORWAY**

Norwegian Defence Research  
Establishment, Attn: Biblioteket  
P.O. Box 25  
NO-2007 Kjeller

**POLAND**

Centralna Biblioteka Wojskowa  
ul. Ostrobramska 109  
04-041 Warszawa

**PORTUGAL**

Estado Maior da Força Aérea  
SDFa – Centro de Documentação  
Alfragide  
P-2720 Amadora

**ROMANIA**

Romanian National Distribution Centre  
Armaments Department  
9-11, Drumul Taberei Street  
Sector 6  
061353 Bucharest

**SLOVAKIA**

Akadémia ozbrojených síl gen  
M.R. Štefánika, Distribučné a  
informačné stredisko STO  
Demänová 393  
031 01 Liptovský Mikuláš 1

**SLOVENIA**

Ministry of Defence  
Central Registry for EU & NATO  
Vojkova 55  
1000 Ljubljana

**SPAIN**

Área de Cooperación Internacional en I+D  
SDGPLATIN (DGAM)  
C/ Arturo Soria 289  
28033 Madrid

**TURKEY**

Milli Savunma Bakanlığı (MSB)  
ARGE ve Teknoloji Dairesi Başkanlığı  
06650 Bakanlıklar – Ankara

**UNITED KINGDOM**

Dstl Records Centre  
Rm G02, ISAT F, Building 5  
Dstl Porton Down, Salisbury SP4 0JQ

**UNITED STATES**

Defense Technical Information Center  
8725 John J. Kingman Road  
Fort Belvoir, VA 22060-6218

**SALES AGENCIES**

**The British Library Document  
Supply Centre**

Boston Spa, Wetherby  
West Yorkshire LS23 7BQ  
UNITED KINGDOM

**Canada Institute for Scientific and  
Technical Information (CISTI)**

National Research Council Acquisitions  
Montreal Road, Building M-55  
Ottawa, Ontario K1A 0S2  
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in “NTIS Publications Database” (<http://www.ntis.gov/>).